ترجمة دورة كالي لينكس المجانية المقدمة من الموقع الرسمي

ترجمة:

علي العمامي

fb.com/al3mamyali

الدورة المجانية لاستكشاف نظام Kali

نصيحة: عندما يقوم مستخدم مسجل بتمييز موضوع الدورة التدريبية على أنه مكتمل، سيتم نقله إلى الموضوع التالي تلقائيًا. إذا قمت بوضع علامة على الدرس بالكامل، فسيأخذك إلى الدرس التالي، حتى لو لم تكن قد انتهيت من جميع الموضوعات. يمكنك بعد ذلك الانتقال إلى العناصر السابقة والتالية التي قرأتها بالفعل.

سيظهر لك أيضًا وضع علامة على درس أو صفحة موضوع مكتملة على تقدمك (يحتاج المستخدمون إلى تسجيل الدخول من أجل مؤشر التقدم هذا)، ويسمح لك بتتبع المكان الذي توقفت عنده.

يمكن استخدام المنتديات لطرح الأسئلة للمساعدة في أي أقسام تواجه صعوبة في فهمها، أو أي تمرين لم ينجح معك كما هو متوقع.

يرجى قراءة والبحث في الكتاب أولاً قبل تجربة أوامر من تمرين أو موضوع، وقبل نشر الأسئلة. إذا كنت لا تزال تواجه مشكلات، فقم بنشر سؤالك بالتفصيل في المنتديات، جنبًا إلى جنب مع بناء جملة الأمر الذي تستخدمه وأي مخرجات خطأ تراه على وحدة التحكم الخاصة بك.

---((نبذة مختصرة))---

يتكون Kali Linux من العديد من الأدوات القوية، ولكن لا يمكنك استخدامها بشكل جيد إذا لم تتقن نظام التشغيل الأساسي. يغطي هذا الكتاب كل ما تحتاج معرفته حتى تتمكن من استخدام Kali Linux ونشره بفعالية.

سيناقش هذا الكتاب الاستخدام الأساسي لنظام Linux للمبتدئين وإدارة حزم Debian واستخدامها وتثبيت Kali والتكوين والأمان والاستخدام المتقدم لنظام Kali بما في ذلك مدى ملاءمة Kali للمؤسسة، ودور Kali في مختلف مراحل تقييم الأمان.

سيكون بمثابة مقدمة للمبتدئين على نظام Kali ولكن أيضًا لتلبية احتياجات المستخدمين الذين يتابعون شهادات Kali والمستخدمين المتقدمين الذين يبحثون عن المزيد من حالات الاستخدام المتعمقة والإلهام.

مقدمة

في عام 1998، كنت أحد المخترقين الناجحين، وشاركت في تأسيس أحد فرق الاختراق البيضاء الأولى المحترفة. كنا أطفالًا، بالفعل، نمتلك وظائف يحلم بها، يدفع لنا لاقتحام بعض أنظمة الحاسوب والشبكات والمباني الأكثر أمانًا على هذا الكوكب.

يبدو الأمر مثيرًا للغاية، ولكن في الواقع، لقد أمضينا معظم وقتنا على لوحة مفاتيح مسلحة بالأدوات الرقمية في عملنا. لقد استخدمنا مجموعة كبيرة من البرامج، التي صممت لتعيين الشبكات وتحديد الأهداف؛ ثم مسحها واستغلالها. في بعض الحالات، يقوم أحدنا (غالبًا Jim Chapple) بكتابة أدوات مخصصة للقيام بأشياء شريرة مثل فحص شبكة من الفئة A (شيء لا تستطيع أي أداة أخرى القيام به في ذلك الوقت)، ولكن في أغلب الأحيان سوف نستخدم أو نعدل الأدوات التي كتبها مجتمع المخترقين. في تلك الأيام التي سبقت Google، ترددنا على BugTraq وAstaLaVista وStorm Packet وw00٠٠w وSecurityFocus وX-Force وغيرها من الموارد لإجراء البحوث وبناء ترسانتنا.

منذ أن كان لدينا وقت محدود في كل حفلة، كان علينا التحرك بسرعة. هذا يعني أننا لا نستطيع قضاء الكثير من الوقت في تجربة الأدوات. كان هذا يعني أننا يجب أن نتعلم الأدوات الأساسية من الداخل والخارج، وحفظ الأدوات المساعدة بحيث نصل إليها بنقرة. لقد كان هذا يعني أنه كان علينا أن نوفر أدواتنا منظمة بشكل جيد، وموثقة، ومختبرة، لذلك ستكون هناك بعض المفاجآت في هذا المجال. بعد كل شيء، إذا لم ندخل، فقدنا وجهنا مع عملائنا وسيأخذون توصياتنا بجدية أقل.

وبسبب هذا، قضيت الكثير من الوقت في فهرسة الأدوات. عندما تم إصدار أداة أو تحديثها، كنت أذهب إلى روتين. كان عليّ معرفة ما إذا كان سيتم تشغيله على منصة الهجوم (بعضها لم يكن كذلك)، وما إذا كان الأمر يستحق ذلك (لم يكن البعض)؛ اضطررت إلى تحديث أي نصوص تعتمد عليها وتوثيقها واختبارها، بما في ذلك ترحيل أي تغييرات تم إجراؤها على الإصدار السابق.

بعد ذلك، أود التخلص من جميع الأدوات ووضعها في المجلدات بناءً على الغرض منها أثناء التقييم. أود كتابة برامج نصية مجمعة لأدوات معينة، وسلاسل بعض الأدوات معًا، وربط كل ذلك في قرص مضغوط منفصل يمكن أن نأخذه في مناطق حساسة، عندما لا يسمح لنا العملاء بأخذ آلات الهجوم أو إزالة الوسائط من مختبراتهم.

كانت هذه العملية مؤلمة، لكنها كانت ضرورية. كنا نعلم أن لدينا القدرة على اقتحام أي شبكة — إذا طبقنا مهاراتنا وخبراتنا بشكل صحيح، ظللنا منظمين، وعملنا بكفاءة. على الرغم من أن البقاء غير مهزوم كان حافزًا، فقد كان يتعلق بتوفير خدمة للعملاء الذين يحتاجون إلينا لاقتحام الشبكات، حتى يتمكنوا من سد الثغرات وتحويل الأموال إلى برامج أمنية.

قضينا سنوات في شحذ مهاراتنا وخبراتنا لكننا لن ننجح دون تنظيم وكفاءة. كنا سنفشل إذا لم نتمكن من وضع أيدينا على الأداة المناسبة عند الحاجة لها.

لهذا السبب قضيت الكثير من الوقت في البحث والتوثيق والاختبار وفهرسة الأدوات، وفي نهاية القرن الحادي والعشرين، سرعان ما أصبحت وظيفة ساحقة بدوام كامل. بفضل الإنترنت، انفجر سطح الهجوم في جميع أنحاء العالم وزاد تنوع وعدد أدوات الهجوم بشكل كبير، كما زاد عبء العمل المطلوب لصيانتها.

ابتداء من عام 2004، لم ينفجر الإنترنت فقط كأساس للأعمال التجارية ولكن أيضًا كمنصة اجتماعية. كانت أجهزة الحاسوب بأسعار معقولة، وأكثر ملاءمة للمستهلكين في كل مكان. توسعت تقنية التخزين من ميغابايت إلى غيغابايت. قفزت الإيثرنت من مئات الكيلوبايت إلى عشرات ميقابايتات في الثانية، وكانت اتصالات الإنترنت أسرع وأرخص من أي وقت مضى. التجارة الإلكترونية آخذة في الازدياد، ومواقع التواصل الاجتماعي مثل (2004) Facebook و (2006) Twitter أصبحت على الإنترنت ونضجت (1998) Google إلى درجة أن أي شخص (بما في ذلك المجرمين) يمكن أن يجد أي شيء على الإنترنت.

نتيجة لذلك، أصبح البحث حاسماً بالنسبة لفرق مثل فرقنا لأنه كان علينا مواكبة الهجمات وأدوات العمل الجديدة. لقد استجبنا لمزيد من جرائم الحاسوب، وطلب عمل التحقيقات الجنائية بأن نخطو قليلاً لأننا استخفنا بالأدلة المحتملة. يعني مفهوم القرص المضغوط المباشر أننا يمكن أن نؤدي التحقيق الجنائي المباشر على جهاز بدون خطر ودون المساس بالأدلة.

الآن أصبح على فريقنا الصغير إدارة أدوات الهجوم وأدوات التحقيق الجنائي؛ كان علينا مواكبة جميع منهجيات الهجوم واستغلالها؛ وكان علينا، كما تعلمون، فعل ما فعلناه مقابل اختبارات الاختراق، التي كانت مطلوبة بشدة. كانت الأمور تخرج عن نطاق السيطرة، وقبل وقت طويل، كنا نقضي وقتاً أقل في المعركة والمزيد من الوقت في البحث، وشحذ أدواتنا، والتخطيط.

لم نكن وحدنا في هذا الصراع. في عام 2004، أصدر Mati "Muts" Aharoni، أحد المخترقين والمتخصصين في مجال الأمن ("WHoppiX" (White hat Knoppix، وهو قرص مضغوط مباشر على نظام Linux والذي وصفه بأنه "القرص المضغوط المباشر لاختبار الاختراق"، وقد تضمن "جميع الاستغلالات من SecurityFocus، Packet Storm وk-otik، إطار عمل Metasploit 2.2 والكثير الكثير. "

أتذكر تنزيل WHoppiX وأنه كان رائعا. لقد قمت بتنزيل أقراص مضغوطة مباشرة أخرى، معتقدًا أنه إذا كنت في حالة قرصنة حقيقية، فستتمكن الأقراص المضغوطة المباشرة من حفظ الـ bacon في الحقل. لكنني لم أكن على وشك الاعتماد على WHoppiX أو أي قرص مضغوط آخر للعمل الحقيقي. لم أثق في أي منهم لتلبية معظم احتياجاتي؛ لم أشعر بأن أي منهم مناسب لسير عملي؛ لم تكن توزيعات كاملة وقابلة للتثبيت؛ وفي اللحظة التي قمت بتنزيلها، كانت قديمة.

لقد أضفت ببساطة هذه الصور المضغوطة، على الرغم من حجمها الهائل نسبيًا، إلى ترسانتنا واستمريت في العملية المؤلمة المتمثلة في الحفاظ على مجموعة الأدوات "الحقيقية" الخاصة بنا.

ولكن على الرغم من آرائي الشخصية في ذلك الوقت، وربما على الرغم من توقعات Muts، كان لـ WHoppiX وتفرعاته تأثير زلزالي على حياته وعلى عملنا ومجتمعنا.

في عام 2005، تطورت WHoppiX إلى WHAX، من خلال مجموعة أدوات موسعة ومحدثة، تستند إلى "القرص المباشر الأكثر حداثة (Slackware) SLAX ". بدا أن Muts وفريق كبير من المتطوعين من مجتمع الاختراق يدركون أنه بصرف النظر عن مدى ثقتهم، لا يمكنهم أبدًا توقع كل نمو وتقلبات عملنا وأن مستخدمي القرص المضغوط لديهم احتياجات متنوعة في هذا المجال. كان من الواضح أن Muts وفريقه كانوا يستخدمون بالفعل WHAX في هذا المجال، ويبدو أنهم ملتزمون بإنجاحه. كان هذا مشجعا بالنسبة لي.

في عام 2006، دمج Muts و Max Moser وفرقهم Auditor Security Linux و WHAX في توزيعة واحدة تسمى BackTrack. لا يزال BackTrack يعتمد على SLAX، حيث استمر في النمو، مضيفًا المزيد من الأدوات والمزيد من الإطارات ودعم اللغة الموسعة والدعم اللاسلكي

المكثف وبنية قائمة تلبي احتياجات المستخدمين المبتدئين والمحترفين ونواة معدلة بشكل كبير. أصبح BackTrack هو التوزيع الأمني الرائد، لكن كثيرين ما زالوا يستخدمونه كنسخة احتياطية لـ "أدواتهم الحقيقية".

بحلول أوائل عام 2009، كان Muts وفريقه قد قاموا بتوسيع BackTrack بشكل ملحوظ إلى BackTrack 4. والآن، أصبح العمل متفرغًا في Muts، ولم يعد BackTrack قرصًا مضغوطًا مباشرًا، بل كان توزيعًا كاملاً يستند إلى Ubuntu مستفيدًا من مستودعات برامج Ubuntu. شهد التحول تطوراً مشهودا: لدى آلية تحديث BackTrack 4. بكلمات Muts الخاصة: "عند المزامنة مع حزم BackTrack الخاصة بنا، سنحصل بانتظام على تحديثات لأدوات الأمان بعد إصدارها بوقت قصير".

كانت هذه نقطة تحول. قام فريق BackTrack بالتحكم في المشاكل التي تواجه مختبري الاختراق ومحللي التحقيق الجنائي وغيرهم ممن يعملون في مجالنا. من شأن جهودهم أن تنقذنا ساعات لا تحصى وتوفر أساسًا ثابتًا، مما يسمح لنا بالعودة مرة أخرى إلى المعركة وقضاء المزيد من الوقت في القيام بالأشياء المهمة (والممتعة). نتيجة لذلك، استجاب المجتمع بالتدفق على المنتديات ويكي. كان BackTrack حقًا مجهودًا اجتماعيًا، حيث لا يزال Muts يتصدر هذا المشروع.

أصبح BackTrack 4 أخيرًا منصة للقوة الصناعية، وقد تنفست أنا وآخرين مثلي الصعداء. كنا نعرف من كثب "الألم والمعاناة" الذي كان يتحمله Muts وفريقه، لأننا كنا نراقب ذلك. نتيجة لهذا، بدأ الكثير منا باستخدام BackTrack كأساس أساسي في مجالنا. نعم، ما زلنا ملتزمين بالأدوات، وكتبنا الكود الخاص بنا، وطورنا استغلالاتنا وتقنياتنا، وبحثنا وجربنا لكننا لم نجمع فقط، حدثنا، وتحققنا من صحة وتنظيم الأدوات.

كانت BackTrack 4 R1 و R2 تنقيحات أخرى في عام 2010، مما أدى إلى إعادة إنشاء Backtrack 5 في عام 2011. لا يزال BackTrack قائمًا على Ubuntu، ويحظى باهتمام كبير مع كل إصدار، أصبح BackTrack الآن مشروعًا ضخمًا يتطلب جهدًا تطوعيًا وجهدًا من المجتمع.

ولكن أيضا التمويل. أطلق Muts برنامج Offensive Security (في عام 2006) ليس فقط لتوفير خدمات التدريب واختبار الاختراق ذات المستوى العالمي ولكن أيضًا لتوفير وسيلة للحفاظ على تطور BackTrack، وضمان بقاء BackTrack مفتوح المصدر ومجاني الاستخدام.

واصلت BackTrack نموها وتحسنها خلال عام 2012 (مع R1 و R2 و R3)، مع الحفاظ على نواة Ubuntu وإضافة مئات من الأدوات الجديدة، بما في ذلك أدوات الاستغلال المادي والأجهزة، ودعم VMware، وعدد لا يحصى من برامج تشغيل الأجهزة اللاسلكية والعديد من تحسينات الاستقرار و اصلاحات الأخطاء. ومع ذلك، بعد إصدار R3، أصبح تطوير BackTrack هادئًا نسبيًا، وبشكل غامض إلى حد ما.

كان هناك بعض التكهنات في هذه الصناعة. اعتقد البعض أن شركة BackTrack بيعت، كانت شركة Offensive Security تتحول إلى واحدة من أكثر شركات التدريب احتراماً وشهرة في مجالنا، وتوقع البعض أن نجاحها قد استحوذ على مطوري BackTrack الرئيسيين وتجاهلهم. ومع ذلك، لا شيء يمكن أن يكون أبعد عن الحقيقة.

في عام 2013، تم إصدار Kali Linux 1.0. من ملاحظات الإصدار: "بعد عام من التطوير الصامت، تفخر Offensive Security بالإعلان عن إطلاق Kali Linux وتوافره على نطاق واسع، وهو التوزيع الأكثر تطوراً وقوةً واستقرارًا لاختبار الاختراق. Kali هي أكثر نضجا وآمنة ومؤسسة من BackTrack. "

Kali لم يكن مجرد إعادة صياغة للعلامة التجارية BackTrack. لقد كان فيها أكثر من 600 أداة، من الواضح أنها مجموعة أدوات رائعة، ولكن لا يزال هناك الكثير منها. تم بناء Kali، من

الألف إلى الياء، على قلب Debian. قد لا يبدو هذا شيئ كبير. لكن آثاره كان مذهل. بفضل جهد إعادة التعبئة الهائل، يمكن لمستخدمي Kali تنزيل المصدر لكل أداة على حدة؛ يمكنهم تعديل وإعادة بناء أداة حسب الحاجة، مع بضع ضغطات المفاتيح فقط. على عكس أنظمة التشغيل الرئيسية الأخرى اليوم، تزامن Kali Linux مع مستودعات Debian أربع مرات في اليوم، مما يعني أنه يمكن لمستخدمي Kali الحصول على تحديثات الحزمة الحالية وإصلاحات الأمان. قام مطورو Kali بالتجربة والتعبئة والمحافظة على الإصدارات الأولية للعديد من الأدوات بحيث ظل المستخدمون دائمًا يحصلون على التحديثات الجديدة. بفضل جذور Debian، يمكن لمستخدمي Kali بدء تثبيت أو تشغيل صورة ISO مباشرة من المستودعات، مما فتح الباب أمام عمليات تثبيت Kali المخصصة بالكامل أو عمليات النشر الضخمة للمؤسسة، والتي يمكن أن تتم أتمتتها وتخصيصها بشكل أكبر مع ملفات ما قبل البذور. لإكمال التخصيص، يمكن لمستخدمي Kali تعديل بيئة سطح المكتب وتعديل القوائم وتغيير الأيقونات وحتى تغيير بيئات النوافذ. فتحت دفعة هائلة لتطوير ARM الباب لتثبيت Kali Linux على مجموعة واسعة من منصات الأجهزة بما في ذلك نقاط الوصول وأجهزة الحواسيب أحادية اللوحة (Raspberry Pi و ODROID و BeagleBone و CubieBoard، على سبيل المثال) **وأجهزة Chromebook المستندة إلى ARM.** وأخيراً وليس آخراً، قامت Kali Linux بتحديثات بسيطة وكبيرة غير ملحوظة مما يعني أنه لن يضطروا أبدًا إلى إعادة تثبيت إعدادات Kali Linux المخصصة.

في الأيام الخمسة الأولى، قام 90.000 منا بتنزيل Kali 1.0.

هذه كانت البداية فقط. في عام 2015، تم إصدار Kali 2.0، تليها الإصدار المستمر عام 2016. باختصار، "إذا كان Kali 1.0 يركز على بناء بنية تحتية قوية، فإن Kali 2.0 يركز على إصلاح تجربة المستخدم والحفاظ على مستجدات الحزم ومستودعات الأدوات".

الإصدار الحالي من Kali Linux هو توزيع مستمر (Rolling)، والذي يمثل نهاية الإصدارات الثابتة. الآن، يتم تحديث المستخدمين باستمرار ويتلقون تحديثات وتصحيحات فور إنشائها. يتم تحديث الأدوات الأساسية بشكل دوري، وتم توفير تحسينات في إمكانية الوصول للمعاقين بصريًا، ويتم تحديث وتصحيح نواة Linux لمواصلة دعم الحقن اللاسلكية 802,11. تضيف أدوات (SDR) واتصال المجال القريب (NFC) دعمًا للحقول الجديدة لاختبار الأمان. تتوفر خيارات التثبيت الكامل للقرص المشفر لنظام Linux **وخيارات التدمير الذاتي لحالات الطوارئ،** وذلك بفضل LVM وLUKS على التوالي، وتمت إضافة خيارات ثبات USB، مما يسمح بتثبيت Kali المستندة إلى USB للحفاظ على التغييرات بين إعادة التشغيل، سواء كان محرك أقراص USB مشفرًا أم لا. أخيرًا، فتحت الإصدارات الحديثة من Kali الباب لـ NetHunter، وهو نظام تشغيل مفتوح المصدر من الطراز العالمي يعمل على الأجهزة المحمولة القائمة على Kali Linux وAndroid.

لقد تطورت Kali Linux ليس فقط إلى نظام الاختبار المحترف في أمن المعلومات، بل إلى نظام تشغيل عالمي وناضج وآمن وجاهز للمؤسسات.

من خلال عملية التطوير التي استمرت لعقد من الزمن، تحمل Muts وفريقه، إلى جانب التفاني الدؤوب من عدد لا يحصى من المتطوعين من مجتمع المخترقين، عبء تبسيط وتنظيم بيئة عملنا، وتحريرنا من الكثير من كدح عملنا وتوفير أساس آمن وموثوق، مما يسمح لنا بالتركيز على دفعنا إلى الأمام نحو الهدف النهائي المتمثل في تأمين عالمنا الرقمي.

ومن المثير للاهتمام، ولكن ليس من المستغرب، أن مجتمعًا مدهشًا قد بنى Kali Linux. كل شهر، ثلاثة إلى أربعمائة ألف منا ينزلون نسخة من Kali. نجتمع معًا في منتديات Kali، التي يبلغ عددهم أربعين ألف شخص، ويمكن العثور على ثلاث إلى أربعمائة منا في وقت واحد على قناة

Kali. نجتمع في المؤتمرات وحضور Kali Dojos لمعرفة كيفية الاستفادة من Kali بشكل أفضل من المطورين أنفسهم.

غير Kali Linux عالم أمن المعلومات للأفضل، وقد أنقذ Muts وفريقه كل واحد منا ساعات لا تحصى من الكد والإحباط، مما سمح لنا بقضاء المزيد من الوقت والطاقة في دفع إنتاجنا للأمام، معًا.

لكن على الرغم من قبولها ودعمها وشعبيتها المذهلة، لم تصدر Kali دليلًا رسميًا. حسنا، الآن بعد أن تغير. يسرني أن أكون إلى جانب فريق التطوير Kali وبالتحديد Mati Aharoni و Raphaël Hertzog و Devon Kearns و Jim O’Gorman لتقديم هذا، وهو الأول في سلسلة من المنشورات الرسمية التي ربما تركز على Kali Linux. في هذا الكتاب، سنركز على منصة Kali Linux نفسها، وسنساعدك على فهم وتعظيم استخدام Kali من الألف إلى الياء. لن نتعمق في ترسانة الأدوات الموجودة في Kali Linux، ولكن سواء كنت مخضرمًا أو مبتدئا، فهذا هو أفضل مكان للبدء، إذا كنت جاهزًا للدخول والحصول على تجربة جدية مع Kali Linux. بغض النظر عن المدة التي قضيتها في التجربة، فإن قرارك بقراءة هذا الكتاب يربطك بمجتمع Kali Linux المتنامي، أحد أقدم وأكبر وأكثر نشاطًا وحيوية في مجالنا.

نيابة عن Muts وبقية فريق Kali المذهل، تهانينا على اتخاذ الخطوة الأولى لإتقان Kali Linux!

جوني لونج

فبراير 2017

---((مقدمة لنظام Kali Linux))---

مقدمة

Kali Linux هي أقوى وأشهر منصة للاختراق في العالم، ويستخدمها متخصصو الأمن في مجموعة واسعة من التخصصات، بما في ذلك اختبار الاختراق، والتحقيق الجنائي، والهندسة العكسية، وتقييم الثغرات الأمنية. إنها تتويجا لسنوات من التحسينات ونتيجة للتطور المستمر للمنصة، من WHoppiX إلى WHAX، إلى BackTrack، والآن إلى إطار اختبار الاختراق الكامل الذي يستفيد من العديد من ميزات Debian GNU / Linux ومجتمع المصادر المفتوحة النابضة بالحياة في جميع أنحاء العالم.

لم يتم تصميم Kali Linux ليكون مجموعة بسيطة من الأدوات فقط، بل هو إطار مرن يمكن لمهنيين اختبار الاختراق المحترفين وعشاق الأمن والطلاب والهواة تخصيصه ليلائم احتياجاتهم الخاصة.

١. لماذا هذا الكتاب؟

Kali Linux ليس مجرد مجموعة من أدوات أمان المعلومات المختلفة التي يتم تثبيتها على قاعدة Debian القياسية وتم تكوينها مسبقًا للحصول على أحدث المعلومات وتشغيلها على الفور. للحصول على أقصى استفادة من Kali، من المهم أن يكون لديك فهم شامل لأسس GNU / Debian Linux القوية (التي تدعم جميع تلك الأدوات الرائعة) وتعلم كيف يمكنك استخدامها في بيئتك.

على الرغم من أن Kali متعددة الأغراض، إلا أنها مصممة بشكل أساسي للمساعدة في اختبار الاختراق. الهدف من هذا الكتاب ليس فقط مساعدتك على الشعور بأنك في بيتك عند استخدام Kali Linux، ولكن أيضًا للمساعدة في تحسين فهمك وتبسيط تجربتك، بحيث عندما تشارك في اختبار الاختراق ويكون الوقت ضروريًا، لا داعي للقلق بشأن فقدان دقائق ثمينة لتثبيت برنامج جديد أو تمكين خدمة شبكة جديدة. في هذا الكتاب، سنقدمك أولاً إلى Linux، ثم سنغطس بشكل أعمق ونحن نقدم لك الفروق الدقيقة الخاصة بـ **Kali Linux** حتى تعرف بالضبط ما يجري تحت الغطاء.

هذه معرفة لا تقدر بثمن، لا سيما عندما تحاول العمل في ظل قيود زمنية ضيقة. ليس من غير المألوف طلب هذا العمق من المعرفة عندما تقوم بالإعداد، أو استكشاف الأخطاء وإصلاحها، أو تكافح لثني أداة لإرادتك، أو تحليل الناتج من أداة، أو الاستفادة من Kali في بيئة واسعة النطاق.

2. هل هذا الكتاب يناسبك؟

إذا كنت تريد الغوص في مجال أمن المعلومات الثري بشكل لا يصدق، وقمت باختيار Kali Linux بحق كمنصة أساسية، فإن هذا الكتاب سيساعدك في هذه الرحلة. تم كتابة هذا الكتاب لمساعدة مستخدمي Linux لأول مرة، وكذلك مستخدمي Kali الحاليين الذين يسعون إلى تعميق معرفتهم بأساسات Kali، وكذلك أولئك الذين استخدموا Kali لسنوات لكنهم يتطلعون إلى إضفاء الطابع الرسمي على تعلمهم، وتوسيع نطاقهم استخدام Kali، وملء الثغرات في معرفتهم.

بالإضافة إلى ذلك، يمكن أن يكون هذا الكتاب بمثابة خارطة طريق ومرجع فني ودليل دراسة لمن يتبعون شهادة Kali Linux Certified Professional "KLCP".

3. النهج العام وهيكل الكتاب

تم تصميم هذا الكتاب بحيث يمكنك وضع يديك على Kali Linux من البداية. ليس عليك قراءة نصف الكتاب للبدء. تتم تغطية كل موضوع بطريقة عملية للغاية، والكتاب مليء بالعينات ولقطات الشاشة للمساعدة في جعل التفسيرات مفهومة أكثر.

الفصل ١: حول Kali Linux، يعرف بعض المصطلحات الأساسية ويشرح الغرض من Kali Linux.

الفصل ٢: "بدء استخدام Kali Linux" يرشدك خطوة بخطوة من تنزيل صورة ISO إلى تشغيل Kali Linux على الحاسوب الخاص بك.

الفصل ٣: أساسيات Linux التي تحتاج لمعرفتها عن أي نظام Linux، مثل بنيته، وعملية التثبيت، والتسلسل الهرمي لنظام الملفات، والأذونات، وأكثر من ذلك. في هذه المرحلة، ستستخدم Kali Linux كنظام مباشر لفترة من الوقت.

الفصل ٤: تثبيت Kali Linux يوضح لك كيفية إجراء تثبيت Kali Linux دائم (على القرص الثابت الخاص بك).

الفصل ٥: تكوين Kali Linux وكيفية تغييره حسب رغبتك. كمستخدم منتظم لـ Kali، فقد حان الوقت للتعرف على الموارد المهمة المتاحة لمستخدمي Kali.

الفصل ٦: الحصول على المساعدة، يمنحك المفاتيح للتعامل مع المشاكل غير المتوقعة التي من المحتمل أن تواجهها.

مع الأساسيات المغطاة جيدًا، يغطس باقي الكتاب في موضوعات أكثر تقدمًا:

الفصل ٧: تأمين ومراقبة Kali Linux يمنحك نصائح للتأكد من أن تثبيت Kali Linux يفي بمتطلبات الأمان الخاصة بك.

الفصل ٨: يشرح إدارة حزم Debian كيفية الاستفادة من الإمكانات الكاملة لنظام التغليف في Debian.

الفصل ٩: Advanced Usage، تتعلم كيفية إنشاء صورة Kali Linux ISO مخصصة بالكامل. كل هذه المواضيع تكون أكثر صلة عندما تقوم بنشر Kali Linux على نطاق واسع في مؤسسة كما هو موثق في **الفصل ١٠**، Kali Linux في المؤسسة.

الفصل الأخير - الفصل ١١، مقدمة في تقييمات الأمان - يجعل الرابط بين كل ما تعلمته في هذا الكتاب والعمل اليومي لمحترفي الأمن.

يعد العمل في هذا الكتاب أيضًا فرصة رائعة قدمها لي ماتي. إنه ليس نفس النوع من العمل، لكن من المفيد بنفس القدر أن نكون قادرين على مساعدة الناس ومشاركتهم خبرتي في نظام التشغيل Kali / Debian. بناءً على تجربتي مع كتيب إدارة Debian، آمل أن تساعدك توضيحاتي على البدء في عالم سريع الحركة لأمن الحاسوب.

---((الفصل الأول))---

1. حول Kali linux

Kali Linux هي توزيعة Linux للتدقيق الأمني جاهزة للشركات تستند على Debian GNU / Linux. يهدف Kali إلى متخصصي الأمن ومسؤولي تقنية المعلومات، مما يمكنهم من إجراء اختبارات الاختراق المتقدمة والتحقيق الجنائي وتدقيق الأمان.

ما هي توزيعات لينكس؟

على الرغم من أنه يستخدم بشكل شائع كاسم لنظام التشغيل بالكامل، إلا أن Linux هو مجرد اسم للنواة (kernel) فقط، وهو برنامج يربط بين الهاردوير وتطبيقات المستخدم النهائي.

يشير مصطلح توزيعة Linux، من ناحية أخرى، إلى نظام تشغيل كامل مبني على نواة Linux، وعادة ما يتضمن برنامج تثبيت والعديد من التطبيقات، إما مثبتة مسبقًا أو مغلفة بطريقة سهلة التثبيت.

Debian GNU / Linux هي إحدى توزيعات Linux الشائعة، معروفة بجودتها واستقرارها. يستند Kali Linux على Debian ويضيف أكثر من 300 حزمة من الأدوات الخاصة، وكلها تتعلق بأمن المعلومات، لا سيما مجال اختبار الاختراق.

Debian هو مشروع برمجي مجاني يوفر إصدارات متعددة من نظام التشغيل الخاص به، وغالبًا ما نستخدم مصطلح التوزيعة للإشارة إلى إصدار محدد منه، على سبيل المثال توزيعات Debian Stable أو Debian Testing. وينطبق الشيء نفسه أيضًا على Kali Linux أيضا – على سبيل المثال Kali Rolling.

1.1 نبذة عن تاريخ Kali

بدأ مشروع Kali Linux بهدوء في عام 2016، عندما قرر Offensive Security أن يحلوا محل مشروع BackTrack Linux الموقر، والذي تمت صيانته يدويًا، بشيء يمكن أن يصبح فرعا من Debian، مع اكمال جميع البنية التحتية المطلوبة وتقنيات التغليف المحسنة. تم اتخاذ القرار لبناء Kali مستندا على Debian؛ لأنه معروف بجودته واستقراره وتوفيره لمجموعة واسعة من البرامج المتاحة. لهذا السبب شارك (Raphaël) في هذا المشروع، كمستشار لديبيان.

حدث الإصدار الأول (الإصدار 1.0) بعد عام واحد، في مارس 2013، واستند على Debian 7 "Wheezy"، التوزيعة الثابتة لـ Debian في ذلك الوقت. في تلك السنة الأولى من التطوير، قمنا بتعبئة مئات التطبيقات المتعلقة باختبار الاختراق وبنينا البنية التحتية. على الرغم من أن عدد التطبيقات كبير، إلا أنه تم تنسيق قائمة التطبيقات بدقة، حيث تم إسقاط التطبيقات التي لم تعد تعمل أو تلك الميزات المكررة المتوفرة بالفعل في برامج أفضل.

خلال العامين التاليين للإصدار 1.0، أصدرت Kali العديد من التحديثات الإضافية، مما أدى إلى توسيع نطاق التطبيقات المتاحة وتحسين دعم الأجهزة، وذلك بفضل إصدارات النواة الأحدث. مع بعض الاستثمار في التكامل المستمر، تأكدنا من أن جميع الحزم المهمة كانت محفوظة في حالة قابلة للتثبيت وأنه يمكن دائمًا إنشاء صور مباشرة مخصصة (خاصية مميزة للتوزيعة).

في عام 2015، عندما خرج "Debian 8 "Jessie، عملنا على إعادة تطبيق Kali Linux. على الرغم من أن Kali Linux 1.x تجنب GNOME Shell (بالاعتماد على GNOME Fallback بدلاً من ذلك)، فقد قررنا في هذا الإصدار احتضانه وتحسينه: لقد أضفنا بعض امتدادات GNOME Shell لاكتساب ميزات مفقودة، وعلى الأخص قائمة التطبيقات. أصبحت نتيجة هذا العمل Kali Linux 2.0، التي نُشرت في أغسطس 2015.

جنوم هي بيئة سطح المكتب الافتراضية لـ Kali linux

كان هذا سابقا أما الأن في نهاية 2019 أصبحتxfce

> تعد بيئة سطح المكتب عبارة عن مجموعة من التطبيقات الرسومية التي تشترك في مجموعة أدوات رسومية شائعة والتي تهدف إلى استخدامها معًا في محطات عمل المستخدم. لا تستخدم بيئات سطح المكتب بشكل عام في الخوادم. وهي توفر عادةً تطبيق shell، مدير ملفات، متصفح ويب، عميل بريد إلكتروني، ومجموعة برامج المكتب، إلخ.

بجانب ذلك قمنا بزيادة جهودنا لضمان حصول Kali Linux دائمًا على أحدث إصدار من جميع تطبيقات اختبار الاختراق. لسوء الحظ، كان هذا الهدف يخالف خصوصيات Debian Stable كقاعدة للتوزيعة، لأنه تطلب منا إعادة دعم العديد من الحزم. هذا يرجع إلى حقيقة أن Debian Stable تضع أولويتها على ثبات البرنامج، وغالبًا ما تتسبب في تأخير طويل من إصدار التحديث الأولي إلى عندما يتم دمجها في التوزيع. نظرًا لاستمرارنا في التكامل المستمر، كان من الطبيعي جدًا إعادة تطبيق Kali Linux على Debian testing حتى نتمكن من الاستفادة من أحدث إصدار من حزم Debian بمجرد توفرها. يحتوي Debian testing على دورة تحديث أكثر قوة، وهو أكثر توافقًا مع أهداف Kali Linux.

هذا، في جوهره، مفهوم Kali Rolling. بينما كان التوزيع المتداول متاحًا لفترة طويلة، فإن Kali 2016.1 كان أول إصدار يحتضن رسميًا الطبيعة المتداولة لهذا التوزيع: عندما تقوم بتثبيت أحدث إصدار من Kali، يتعقب نظامك فعليًا توزيع Kali Rolling وكل يوم تحصل عليه تحديثات جديدة. في الماضي، كانت إصدارات Kali عبارة عن لقطات لتوزيع Debian Stable مع حزم Kali الخاصة التي تم حقنها فيه.

يحتوي التوزيع المستمر "Rolling" على العديد من الفوائد، ولكنه يأتي أيضًا مع تحديات متعددة، سواء بالنسبة للذين يقومون ببناء التوزيعة أو للمستخدمين الذين يضطرون إلى التعامل مع تدفق لا نهائي من التحديثات وأحيانًا إلى تغييرات غير متوافقة مع الإصدارات السابقة. يهدف هذا الكتاب إلى تزويدك بالمعرفة المطلوبة للتعامل مع كل ما قد تواجهه أثناء إدارة تثبيت Kali Linux.

2.1. علاقة Kali بـ Debian

تستند توزيعة Kali Linux على Debian testing. لهذا، تأتي معظم الحزم المتوفرة في Kali Linux مباشرة من مستودع Debian هذا.

بينما تعتمد Kali Linux اعتمادًا كبيرًا على Debian، فهي أيضًا مستقلة تمامًا، بمعنى أن لدينا بنية تحتية خاصة بنا ونحتفظ بحرية إجراء أي تغييرات نريدها.

1.2.1. تدفق الحزم

من جانب Debian، يعمل المطورون كل يوم على تحديث الحزم وتحميلها على توزيعة Debian unstable. من هناك، تنتقل الحزم إلى توزيع Debian testing بمجرد التخلص من أكثر الأخطاء إثارة للمشاكل. تضمن عملية الترحيل أيضًا عدم كسر التبعيات في Debian testing. الهدف هو أن الاختبار يكون دائمًا في حالة قابلة للاستخدام (أو حتى يمكن إعادة تشغيله!).

تتوافق أهداف Debian testing جيدًا مع أهداف Kali Linux، لذا اخترناها كقاعدة.

لإضافة الحزم الخاصة بـ Kali في التوزيعة، نتبع عملية من خطوتين.

أولاً، نأخذ Debian testing ونحقن حزم Kali الخاصة بنا فيه (الموجودة في مستودع kali-dev-only) لبناء مستودع kali-dev. ستتوقف هذا الحزم من وقت لآخر: على سبيل المثال، قد لا تكون حزم Kali الخاصة بنا قابلة للتثبيت حتى يتم إعادة تجميعها مقابل المكتبات الأحدث. في حالات أخرى، قد يلزم أيضًا تحديث الحزم التي قمنا بتشكيلها، إما لتصبح قابلة للتثبيت مرة أخرى، أو لإصلاح قابلية تثبيت حزمة أخرى تعتمد على إصدار أحدث من الحزمة forked. في أي حال، ليست kali-dev للمستخدمين النهائيين.

2.2.1. إدارة الفرق مع Debian

كقرار تصميم، نحاول تقليل عدد الحزم المتفرعة إلى أقصى حد ممكن. ومع ذلك، من أجل تنفيذ بعض الميزات الفريدة لـKali، يجب إجراء بعض التغييرات.

للحد من تأثير هذه التغييرات، نحن نسعى جاهدين لإرسالها في مرحلة أخرى، إما عن طريق دمج الميزة مباشرة، أو عن طريق إضافة الروابط المطلوبة بحيث يكون من السهل تمكين الميزات المطلوبة دون مزيد من تعديل الحزم الأولية نفسها.

يساعدنا Kali Package Tracker على تتبع اختلافاتنا مع Debian. في أي وقت، يمكننا البحث عن الحزمة التي تفرعت وما إذا كانت متزامنة مع Debian أو لا، أو إذا كان التحديث مطلوباً أو لا. يتم الاحتفاظ بكل حزمنا في مستودعات Git التي تستضيف فرع Debian وفرع Kali جنباً إلى جنب. وبفضل هذا، فإن تحديث حزمة متفرعة هو عملية بسيطة من خطوتين: تحديث فرع Debian ثم دمجها في فرع Kali.

في حين أن عدد الحزم المتفرعة في Kali منخفضة نسبياً، فإن عدد الحزم الإضافية مرتفع إلى حد ما: في أبريل 2017 كان هناك ما يقرب من 400 حزمة. معظم هذه الحزم عبارة عن برامج مجانية تتوافق مع إرشادات Debian للبرمجيات الحرة وسيكون هدفنا النهائي هو الحفاظ على تلك الحزم في Debian متى ما أمكن ذلك. لهذا السبب نسعى جاهدين لامتثال سياسة Debian واتباع ممارسات التعبئة الجيدة المستخدمة في Debian. لسوء الحظ، هناك أيضًا بعض الاستثناءات القليلة التي كان من المستحيل إنشاء التغليف المناسب فيها. نتيجة لضيق الوقت، تم دفع عدد قليل من الحزم إلى Debian.

3.1. الغرض منه وحالات استخدامه

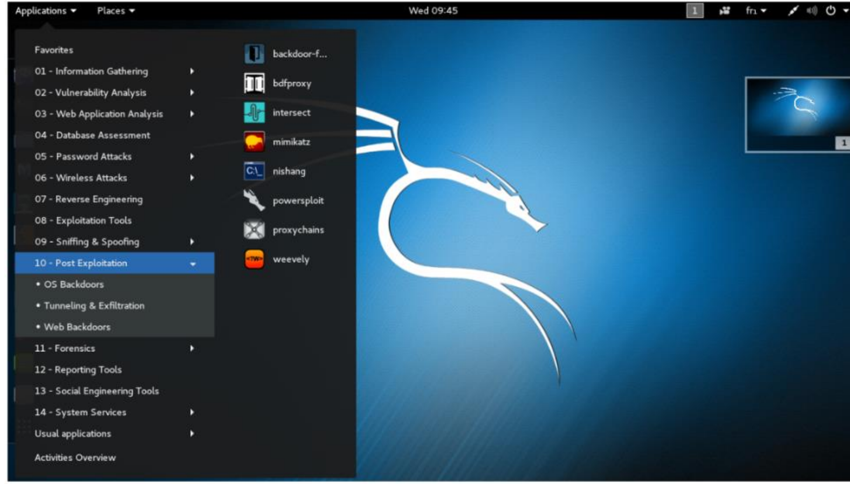
بينما يمكن تلخيص تركيز Kali باختصار على أنه "اختبار الاختراق والتدقيق الأمني"، هناك العديد من المهام المختلفة التي تنطوي عليها هذه الأنشطة. تم تصميم Kali Linux كإطار عمل، لأنه يشتمل على العديد من الأدوات التي تغطي حالات استخدام مختلفة تمامًا.

على سبيل المثال، يمكن استخدام Kali Linux على أنواع مختلفة من أجهزة الحاسوب: بالتأكيد أجهزة الحاسوب المحمولة، وأيضًا على خوادم مسؤولي النظام الذين يرغبون في مراقبة شبكاتهم، وعلى محطات عمل محللي التحقيق الجنائي، وبشكل غير متوقع، على الأجهزة المضمنة المخفية، عادةً مع وحدات المعالجة المركزية ARM، التي يمكن إسقاطها في نطاق شبكة لاسلكية أو توصيلها في جهاز الحاسوب الخاص بالمستخدمين المستهدفين. العديد من أجهزة ARM هي أيضًا آلات هجوم مثالية نظرًا لحجمها الصغير ومتطلبات الطاقة المنخفضة.

يمكن أيضًا نشر Kali Linux في السحابة لإنشاء مجموعة من آلات تكسير كلمة المرور، وعلى الهواتف المحمولة والأجهزة اللوحية للسماح باختبار الاختراق المحمول بحق.

ولكن هذا ليس كل شيء؛ يحتاج اختبار الاختراق أيضًا إلى خوادم: لاستخدام برنامج تعاون ضمن فريق من اختبار الاختراق، لإعداد خادم ويب لاستخدامه في حملات التصيد الاحتيالي، لتشغيل أدوات مسح الثغرات الأمنية وغيرها من الأنشطة ذات الصلة.

بمجرد تشغيل Kali، ستكتشف بسرعة أن قائمة Kali Linux الرئيسية مرتبة حسب الخاصيات حسب مختلف أنواع المهام والأنشطة ذات صلة بمختبري الاختراق وغيرهم من متخصصي أمن المعلومات كما هو موضح في الشكل ١.١."قائمة تطبيقات Kali Linux" التالية.



الشكل ١.١. قائمة تطبيقات Kali linux

تشمل هذه المهام والأنشطة:

- ❖ **جمع المعلومات (Information Gathering):** جمع البيانات حول الشبكة المستهدفة وهيكلها، وتحديد أجهزة الحاسوب، وأنظمة التشغيل الخاصة بهم، والخدمات التي يقومون بتشغيلها. تحديد الأجزاء التي يحتمل أن تكون حساسة في نظام المعلومات. استخراج جميع أنواع القوائم من مجلد تشغيل الخدمات.
- ❖ **تحليل الثغرات الأمنية (Vulnerability Analysis):** اختبار ما إذا كان النظام المحلي أو البعيد يتأثر بعدد من الثغرات الأمنية المعروفة أو التكوينات غير الآمنة. تستخدم ماسحات عدم الحصانة قواعد البيانات التي تحتوي على آلاف التواقيع لتحديد نقاط الضعف المحتملة.
- ❖ **تحليل تطبيقات الويب (Web Application Analysis):** تحديد التكوينات الخاطئة والضعف الأمني في تطبيقات الويب. من الضروري تحديد هذه المشكلات وتخفيفها نظراً لأن هذه التطبيقات توفر للجمهور مما يجعلها أهدافاً مثالية للمهاجمين.
- ❖ **تقييم قاعدة البيانات (Database Assessment):** من حقن SQL إلى مهاجمة بيانات الاعتماد، تعد هجمات قاعدة البيانات هدفا شائعًا للغاية للمهاجمين. يمكنك العثور على

الأدوات التي تختبر أهداف الهجوم التي تتراوح من حقن SQL إلى استخراج البيانات وتحليلها هنا.

- ❖ **هجمات كلمة المرور (Password Attacks):** أنظمة المصادقة دائمًا معرضة للهجوم. يمكن العثور هنا على العديد من الأدوات المفيدة، بدءًا من أدوات الهجوم على كلمات المرور عبر الإنترنت إلى الهجمات التي لا تعمل في وضع عدم الاتصال على أنظمة التشفير أو التجزئة.
- ❖ **الهجمات اللاسلكية (Wireless Attacks)**: تعني الطبيعة الواسعة الانتشار للشبكات اللاسلكية أنها ستكون دائمًا هدفا شائعًا للهجوم. بفضل النطاق الواسع من الدعم لبطاقات لاسلكية متعددة، تعد Kali خيارًا واضحًا للهجمات ضد أنواع متعددة من الشبكات اللاسلكية.
- ❖ **الهندسة العكسية (Reverse Engineering):** الهندسة العكسية هي نشاط له أغراض عديدة. دعما للأنشطة الهجومية، فهي واحدة من الطرق الأساسية لتحديد نقاط الضعف واستغلال تطويرها. على الجانب الدفاعي، يتم استخدامها لتحليل البرامج الضارة المستخدمة في الهجمات المستهدفة. في هذه المرحلة، الهدف هو تحديد قدرات قطعة معينة من الحرف اليدوية.
- ❖ **أدوات الاستغلال (Exploitation Tools):** تتيح لك الاستغلال، أو الاستفادة من ثغرة أمنية (تم التعرف عليها سابقًا)، التحكم في آلة بعيدة (أو جهاز). يمكن بعد ذلك استخدام هذا الوصول لمزيد من هجمات تصعيد الامتيازات، إما محليًا على الجهاز المصاب، أو على أجهزة أخرى يمكن الوصول إليها على نفس الشبكة. تحتوي هذه الفئة على عدد من الأدوات والأدوات المساعدة التي تعمل على تبسيط عملية كتابة استغلالاك الخاصة.
- ❖ **الشم والخداع (Sniffing & Spoofing)**: يعد الوصول إلى البيانات أثناء انتقالها عبر الشبكة مفيدًا للمهاجمين. يمكنك هنا العثور على أدوات الخداع التي تتيح لك انتحال شخصية

مستخدم شرعي بالإضافة إلى أدوات شم تسمح لك بالتقاط وتحليل البيانات مباشرةً من السلك. عند استخدامها معًا، يمكن أن تكون هذه الأدوات قوية جدًا.

- ❖ **مرحلة ما بعد الاستغلال (Post Exploitation):** بمجرد حصولك على حق الوصول إلى نظام ما، فإنك تريد غالبًا الحفاظ على هذا المستوى من الوصول أو توسيع نطاق التحكم من خلال التنقل بشكل جانبي عبر الشبكة. الأدوات التي تساعد في تحقيق هذه الأهداف موجودة هنا.
- ❖ **التحقيق الجنائي (Forensics):** كانت بيئات الإقلاع المباشر (التحقيق الجنائي) من لينكس مشهورة للغاية منذ سنوات. يحتوي Kali على عدد كبير من أدوات التحقيق الجنائي الشائعة التي تستند إلى Linux والتي تتيح لك القيام بكل شيء بدءًا من الفرز الأولي وحتى تصوير البيانات والتحليل الكامل وإدارة الحالات.
- ❖ **أدوات إعداد التقارير (Reporting Tools):** لا يكتمل اختبار الاختراق إلا بعد الإبلاغ عن النتائج. تحتوي هذه الفئة على أدوات للمساعدة في تجميع البيانات التي تم جمعها من أدوات جمع المعلومات، واكتشاف العلاقات غير الواضحة، والجمع بين كل شيء في تقارير مختلفة.
- ❖ **أدوات الهندسة الاجتماعية (Social Engineering Tools):** عندما يكون الجانب الفني مضمونًا بشكل جيد من الناحية الدفاعية، غالبًا ما تكون هناك إمكانية لاستغلال السلوك الإنساني كهدف للهجوم. بالنظر إلى التأثير الصحيح، يمكن حث الناس على اتخاذ الإجراءات التي تعرِّض أمن البيئة للخطر. هل يحتوي مفتاح USB الذي وصله السكرتير للتو على ملف PDF غير ضار؟ أم هل كان حصان طروادة أيضًا قام بتثبيت الباب الخلفي؟ هل كان موقع الويب المصرفي هو المحاسب الذي قام للتو بتسجيل الدخول إلى موقع الويب المتوقع أم نسخة كاملة تستخدم لأغراض التصيد؟ تحتوي هذه الفئة على أدوات تساعد في هذه الأنواع من الهجمات.

❖ **خدمات النظام (System Services):** تحتوي هذه الفئة على أدوات تسمح لك ببدء وإيقاف التطبيقات التي تعمل في الخلفية كخدمات للنظام.

4.1. ميزات Kali linux الرئيسية

Kali Linux هي توزيعة Linux تحتوي على مجموعة خاصة من مئات أدوات البرمجيات المصممة خصيصًا للمستخدمين المستهدفين – مختبري الإختراق وغيرهم من متخصصي الأمان-. يأتي أيضًا مع برنامج تثبيت لإعداد Kali Linux بالكامل كنظام تشغيل رئيسي على أي جهاز حاسوب.

يشبه هذا إلى حد كبير جميع توزيعات Linux الأخرى الموجودة، لكن هناك ميزات أخرى تميز Kali Linux، والتي تم تصميم العديد منها لتلبية الاحتياجات المحددة لاختبار الاختراق. دعنا نلقي نظرة على بعض هذه الميزات.

1.4.1. نظام مباشر

على عكس معظم توزيعات Linux، فإن صورة ISO الرئيسية التي تقوم بتنزيلها ليست مخصصة فقط لتثبيت النظام؛ بل يمكنك استخدامها أيضًا كنظام مباشر قابل للإقلاع. بمعنى آخر، يمكنك استخدام Kali Linux دون تثبيته، فقط عن طريق تشغيل صورة ISO (عادةً بعد نسخ الصورة على مفتاح USB).

يحتوي النظام المباشر على الأدوات الأكثر استخداماً في اختبار الاختراق، لذا حتى لو لم يكن نظامك الاساسي هو Kali Linux، يمكنك ببساطة إدخال القرص أو مفتاح USB وإعادة التشغيل لتشغيل Kali. ومع ذلك، ضع في اعتبارك أن التكوين الافتراضي لن يحفظ التغييرات بين عمليات إعادة الإقلاع. إلا إذا قمت بتكوين الثبات باستخدام مفتاح USB (انظر القسم "إضافة الثبات إلى Live ISO باستخدام USB")، يمكنك تعديل النظام حسب رغبتك (تعديل ملفات التهيئة، وحفظ التقارير، وترقية البرامج، وتثبيت حزم إضافية، إلخ ...)، وسيتم الاحتفاظ بالتغييرات حتى بعد إعادة تشغيل الحاسوب.

2.4.1. وضع التحقيق الجنائي

بشكل عام، عند القيام بعمل التحقيق الجنائي على نظام ما، فأنت تريد تجنب أي نشاط من شأنه أن يغير البيانات الموجودة على النظام الذي تم تحليله بأي طريقة. لسوء الحظ، تميل بيئات سطح المكتب الحديثة إلى التداخل مع هذا الهدف من خلال محاولة وصل أي قرص (أقراص) تكتشفها تلقائيًا. لتجنب هذا السلوك، يحتوي Kali Linux على وضع التحقيق الجنائي الذي يمكن تمكينه من قائمة الإقلاع: سيعطل كل هذه الميزات.

يعد النظام المباشر مفيدًا بشكل خاص لأغراض التحقيق الجنائي، لأنه من الممكن إعادة تشغيل أي جهاز حاسوب في نظام Kali Linux دون وصل الأقراص الصلبة أو تعديلها.

3.4.1. تخصيص نواة لينكس

يوفر Kali Linux دائمًا نواة Linux مخصصة حديثًا، استنادًا إلى الإصدار في Debian Unstable. هذا يضمن دعم العتاد (الهاردوير)، وخاصة بالنسبة لمجموعة واسعة من تعريف الأجهزة اللاسلكية. النواة مصححة لدعم الحقن اللاسلكية؛ لأن بعض أدوات تقييم الأمان اللاسلكية تعتمد على هذه الميزة.

نظرًا لأن العديد من الأجهزة تتطلب ملفات برامج ثابتة محدثة (موجودة في /lib/firmware/)، فإن Kali تقوم بتثبيتها جميعًا بشكل افتراضي - بما في ذلك البرامج الثابتة المتوفرة في القسم الغير مجاني في Debian. لم يتم تثبيتها افتراضياً في Debian، لأنها مصدر مغلق وبالتالي فهي ليست جزءًا من Debian.

4.4.1. تخصيص بكل معنى الكلمة

تم تصميم Kali Linux من قِبل مختبري اختراق وهو لمختبري الاختراق، لكننا نتفهم أنه لن يوافق الجميع على قرارات التصميم الخاصة بنا أو اختيار الأدوات التي يجب تضمينها افتراضيًا. مع وضع ذلك في الاعتبار، نحن نضمن دائمًا سهولة تخصيص Kali Linux حسب احتياجاتك وتفضيلاتك. تحقيقًا لهذه الغاية، ننشر تهيئة البناء المباشر المستخدمة في إنشاء صور Kali الرسمية حتى تتمكن من تخصيصها حسب رغبتك. من السهل جدًا البدء في هذا التكوين وتنفيذ تغييرات متنوعة بناءً على احتياجاتك بفضل براعة Live-build.

يتضمن Live-build العديد من الميزات لتعديل النظام المثبت، وتثبيت الملفات الإضافية، وتثبيت حزم إضافية، وتشغيل الأوامر التعسفية (arbitrary commamds)، وتغيير القيم التي تم نقلها مسبقًا إلى debconf.

5.4.1. نظام تشغيل موثوق

يجب على المستخدمين الأمنيين معرفة أنه يمكنهم الوثوق به لأنه تم تطويره في مرأى من الجميع ولأنه يمكن لأي شخص فحص الكود المصدري. تم تطوير Kali Linux بواسطة فريق صغير من المطورين ذوي المعرفة، يعملون بشفافية ويتبعون أفضل ممارسات الأمان: يقومون بتحميل حزم المصدر الموقعة والتي يتم بناؤها بعد ذلك، يتم اختبار الحزم وتوزيعها كجزء من حزم الموقع.

يمكن مراجعة العمل المنجز على الحزم بالكامل من خلال حزم Git للتعبئة والتغليف (التي تحتوي على علامات موقعة) والتي يتم استخدامها لإنشاء حزم مصادر Kali. يمكن أيضًا متابعة تطور كل حزمة من خلال حزم Kali Tracker.

6.4.1. قابلة للاستخدام على مجموعة واسعة من أجهزة ARM

يوفر Kali Linux حزمًا ثنائيةً لبُنْيَات armel و armhf و arm64 ARM. بفضل الصور القابلة للتثبيت بسهولة والتي يوفرها Offensive Security، يمكن نشر Kali Linux على العديد من الأجهزة المثيرة للاهتمام، من الهواتف الذكية والأجهزة اللوحية إلى أجهزة توجيه (Router) Wi-Fi وأجهزة الحاسوب من مختلف الأشكال والأحجام.

5.1. سياسات Kali Linux

بينما تسعى Kali Linux جاهدة إلى اتباع سياسة Debian كلما أمكن ذلك، هناك بعض المجالات التي اتخذنا فيها خيارات تصميم مختلفة إلى حد كبير بسبب الاحتياجات الخاصة لمتخصصي الأمن.

1.5.1. مستخدم جذر واحد افتراضيًا

(*لن يكون هذا مع بداية ٢٠٢٠*) تشجع معظم توزيعات Linux، بشكل معقول، استخدام حساب غير متميز أثناء تشغيل النظام واستخدام أداة مساعدة مثل **sudo** عند الحاجة إلى امتيازات إدارية. هذه نصيحة أمنية سليمة، توفر طبقة إضافية من الحماية بين المستخدم وأي أوامر أو عمليات لنظام تشغيل تحتمل التخريب أو التدمير. ينطبق هذا بشكل خاص على أنظمة المستخدم المتعددة، حيث يكون الفصل بين امتياز المستخدم متطلبًا — فقد يؤدي سوء تصرف أحد المستخدمين إلى تعطيل عمل العديد من المستخدمين أو إتلاف حساباتهم أو إتلاف النظام.

نظرًا لأن العديد من الأدوات المضمنة في Kali Linux لا يمكن تنفيذها إلا بامتيازات الجذر، فهذا هو حساب مستخدم Kali الافتراضي. بخلاف توزيعات Linux الأخرى، لن تتم مطالبتك بإنشاء مستخدم غير متميز عند تثبيت Kali. تمثل هذه السياسة بالذات انحرافًا كبيرًا عن معظم أنظمة Linux وتميل إلى أن تكون مربكة للغاية للمستخدمين الأقل خبرة. يجب على المبتدئين توخي الحذر بشكل خاص عند استخدام Kali لأن معظم الأخطاء المدمرة تحدث عند العمل بامتيازات الجذر.

2.5.1. تم تعطيل خدمات الشبكة بشكل افتراضي

على عكس Debian، يقوم Kali Linux بتعطيل أي خدمة مثبتة تستمع على واجهة شبكة عامة بشكل افتراضي، مثل: HTTP وSSH.

الأساس المنطقي وراء هذا القرار هو تقليل التعرض أثناء اختبار الاختراق عندما يكون من الضار الإعلان عن وجودك والكشف عن المخاطر بسبب تفاعلات الشبكة غير المتوقعة.

لا يزال بإمكانك تمكين أي خدمة عن طريق كتابة الأمر:

```
systemctl enable service
```

سنناقش هذا في الفصل الخامس، تكوين Kali Linux.

3.5.1. مجموعة تطبيقات مختارة

تهدف Debian إلى أن تكون نظام التشغيل العالمي وتضع قيودًا قليلة جدًا على ما يتم تعبئته، شريطة أن يكون لكل حزمة صيانة.

على النقيض من ذلك، لا يقوم Kali Linux بحزم كل أداة لاختبار الاختراق المتاحة. بدلاً من ذلك، نهدف إلى توفير أفضل الأدوات المرخصة بحرية والتي تغطي معظم المهام التي قد يرغب مختبر الاختراق في تنفيذها.

يعمل مطورو Kali الذين يعملون كمختبرين للاختراق على التحكم في عملية الاختيار، ونستفيد من تجاربهم وخبراتهم في اتخاذ خيارات صحيحة.

فيما يلي بعض النقاط التي يتم أخذها في الاعتبار عند تقديم طلب جديد:

- ❖ فائدة التطبيق في مجال اختبار الاختراق
- ❖ الوظيفة الفريدة لميزات التطبيق
- ❖ رخصة التطبيق
- ❖ متطلبات موارد التطبيق

يعد الاحتفاظ بحزم أدوات اختبار الاختراق المحدثة والمفيدة مهمة صعبة. نرحب باقتراحات الأدوات ضمن فئة مخصصة (New Tool Requests) في Kali Bug Tracker. يتم تلقي طلبات الأداة الجديدة على أفضل وجه عندما يتم تقديم المقترح جيدًا، بما في ذلك شرح لمدى فائدة الأداة وكيف تقارن بالتطبيقات الأخرى المشابهة وما إلى ذلك.

6.1. ملخص

في هذا الفصل قدمنا لك Kali Linux، قدمنا نبذة عن تاريخه، وعلى بعض الميزات الأساسية، وحالات الاستخدام. لقد ناقشنا أيضًا بعض السياسات التي اعتمدناها عند تطوير Kali Linux.

نصائح التلخيص:

- ❖ Kali Linux هي توزيعة Linux جاهزة لمراجعة حسابات الشركات، وتستند على Debian GNU / Linux. يهدف Kali إلى المتخصصين في مجال الأمن ومسؤولي تقنية المعلومات، مما يمكنهم من إجراء اختبارات الاختراق المتقدمة والتحقيق الجنائي وتدقيق الأمان.
- ❖ على عكس معظم أنظمة التشغيل الرئيسية، يعد Kali Linux توزيعًا مستمرًا، مما يعني أنك ستتلقى التحديثات كل يوم.
- ❖ تستند توزيعة Kali Linux على Debian testing. لذلك، تأتي معظم الحزم المتوفرة في Kali Linux مباشرة من مستودع Debian هذا.
- ❖ بينما يمكن تلخيص استخدام Kali بسرعة بـ "اختبار الاختراق ومراجعة الأمان"، هناك العديد من حالات الاستخدام، بما في ذلك مسؤولو النظام الذين يرغبون في مراقبة شبكاتهم، وعمل التحقيق الجنائي، وتركيبات الأجهزة المدمجة، والمراقبة اللاسلكية، والتثبيت على المنصات المحمولة، وأكثر من ذلك.
- ❖ تسهل قوائم Kali الوصول إلى الأدوات الخاصة بالمهام والأنشطة المختلفة بما في ذلك: تحليل الثغرات الأمنية، وتحليل تطبيقات الويب، تقييم قواعد البيانات، هجمات كلمة المرور، الهجمات اللاسلكية، الهندسة العكسية، أدوات الاستغلال، الشم والخداع، أدوات ما

بعد الاستغلال، التحقيق الجنائي، أدوات إعداد التقارير، وأدوات الهندسة الاجتماعية، وخدمات النظام.

❖ يحتوي Kali Linux على العديد من الميزات المتقدمة بما في ذلك: الاستخدام كنظام مباشر (غير مثبت)، ووضع التحقيق الجنائي القوي والآمن، ونواة Linux مخصصة، والقدرة على تخصيص النظام بالكامل، ونظام تشغيل أساسي موثوق به وآمن، وإمكانية تثبيت ARM، وسياسات الشبكة الافتراضية الآمنة، ومجموعة من التطبيقات المختارة.

في الفصل التالي، سنبدأ مع بعض أساسيات Linux.

التمرين الأول، للفصل الأول - إعداد بيئتنا

١. قم بإنشاء VM جديد في VMware (اختار Debian 64 bit).
٢. قم بتعيينه على الأقل من ذاكرة الوصول العشوائي (RAM) سعة 2 GB، وحدتي CPU، و 30 GB للقرص الصلب
٣. ربط صورة ISO Kali إلى CDROM الإفتراضي.
٤. تأكد من أن VM في وضع NAT.
٥. قم بتشغيل جهاز VM، وفحص خيارات الإقلاع Kali وفهمها.

غذاء الفكر

١. ما هو إصدار ديبيان Debian التي يستند عليه Kali 1.0 و Rolling 2.0؟
٢. ما هي الاختلافات الرئيسية بين الإقلاع المباشر لـ Kali والمثبت؟
٣. ما الفرق بين وضع الإقلاع المباشر ووضع التحقيق الجنائي؟
٤. كيف يمكننا التحقق من أن وضع التحقيق الجنائي يعمل؟
٥. ما هي أفضل طريقة لإدراج أداة في Kali؟
٦. اسم بعض الميزات الرائعة في Kali؟

الإجابة:

تحقق من كل خيارات الإقلاع. استخدم "tap" لتحرير معلمات الإقلاع في حالة استخدام syslinux أو "e" إذا كنت تستخدم grub.



١. المباشر – الإقلاع المباشر، كالمعتاد.

٢. المباشر (الوضع الآمن) – يقلع بأقل تعريفات للهاردوير والأجهزة. // الأجهزة المطلوبة فقط//

٣. المباشر (التحقيق الجنائي) - يقلع دون وصل أي شيء، ومناسبة لعمل التحقيق الجنائي.

٤. مباشر (ثابت ومشفر) - ما عليك سوى إضافة الأقسام المطلوبة، وقائمة الإقلاع جاهزة للاستمرار.

٥. تثبيت (install) - عادي، بواجهة قديمة

٦. تثبيت رسومي - وضع التثبيت بواجهة المستخدم الرسومية الخاصة بنظام كالي

٧. التثبيت بالنطق - تثبيت Kali للمستخدمين ضعاف البصر.

٨. أداة الكشف عن الأجهزة - مصممة لعرض معلومات الأجهزة ذات المستوى المنخفض.

٩. تشخيص الذاكرة - erm، تشخيص الذاكرة!

إجابات غذاء الفكر

١. يستند Kali 1.0 على Debian Wheezy، بينما Kali 2.0 يستند على Jessie.

٢. يتم تشغيل الوضع المباشر على ذاكرة الوصول العشوائي (RAM) وKali المثبت على ذاكرة تخزين.

٣. يتم تشغيل الوضع المباشر على ذاكرة الوصول العشوائي، ولكن قد يتم تحميل الأقراص تلقائيًا. وضع التحقيق الجنائي لا يقوم بوصل محركات الأقراص تلقائيًا.

٤. استخدم الأمر **mount** للتحقق من عدم تركيب أي أقراص. يمكنك أيضًا استخراج هاش md5 وتبديل النظام وأجهزة الأقراص، وإعادة التشغيل في وضع التحقيق الجنائي واستخراج هاش md5 مرة أخرى. يجب أن يتطابقا الهاشا الـ md5 إذا نجح وضع التحقيق الجنائي. جرب هذا في نظام لا يهمك أن يتغير ما فيه!

٥. أفضل طريقة لطلب إضافة أداة هي فتح تذكرة "New Tool Requests" في Kali Bug Tracker.

٦. نظام مباشر، وضع التحقيق المباشر، نواة لينكس مخصصة، قابلة للتخصيص بالكامل، نظام تشغيل موثوق به مع خدمات الشبكة الافتراضية المعطلة، دعم ARM، أدوات الأمان المحملة مسبقًا، منصة اختبار الاختراق!

اختبار الشهادة للفصل الأول

ما هو أحدث إصدار من Kali:

- توزيع ثابت، يستند على Debian testing Wheezy.
- توزيع ثابت، يستند على Debian Stable Jessie.
- توزيع مستمر، يستند على Debian testing.
- توزيع مستمر، يستند على Debian Stable Wheezy.

الإجابة:

توزيع مستمر، يستند على Debian testing.

A rolling distribution based on Debian testing

---((الفصل الثاني))---

2. البداية مع Kali

على عكس بعض أنظمة التشغيل الأخرى، فإن Kali Linux يجعل البداية سهلة، بفضل حقيقة أن صوره على القرص هي ISOs مباشرة، مما يعني أنه يمكنك تشغيل الصورة التي تم تنزيلها دون اتباع أي إجراء تثبيت مسبق. هذا يعني أنه يمكنك استخدام نفس الصورة للاختبار أو لاستخدامها كصورة USB أو DVD-ROM قابلة للإقلاع في حالة التحقيق الجنائي أو للتثبيت كنظام تشغيل أساسي على أجهزة حقيقية أو افتراضية.

مع هذه البساطة، يجب ألاَّ ننسى أنه يجب اتخاذ بعض الاحتياطات. غالبًا ما يكون مستخدمو Kali هدفًا للذين عندهم نوايا سيئة، سواءً كانت مجموعات تمولها الدول أو عناصر من الجريمة المنظمة أو مخترقين فرديين. بسبب طبيعة Kali Linux (المفتوحة المصدر) من السهل نسبيًا إنشاء إصدارات مزيفة وتوزيعها؛ لذلك من الضروري أن تتعرف على عملية التنزيل من المصادر الأصلية والتحقق من سلامة صورتك التي قمت بتنزيلها. هذا مهم بشكل خاص لمتخصصي الأمن الذين غالبًا ما يمكنهم الوصول إلى الشبكات الحساسة والمكلفين ببيانات العميل.

1.2. تنزيل صورة ISO لنظام كالي

1.1.2. من أين يمكنني الحصول على نظام كالي

المصدر الرسمي الوحيد لصور Kali Linux ISO هو قسم "Downloads" في موقع Kali الإلكتروني.

https://www.kali.org/downloads/

نظراً لشهرته، تقدم العديد من المواقع صور Kali للتنزيل، لكن لا ينبغي اعتبارها جديرة بالثقة قد تكون مصابة بالفعل ببرامج ضارة أو تتسبب في ضرر لا يمكن إصلاحه لنظامك.

الموقع متاح عبر HTTPS، مما يجعل من الصعب انتحال شخصيته. لا تكون القدرة على تنفيذ هجوم رجل في الوسط كافية؛ لأن المهاجم سيحتاج أيضًا إلى شهادة www.kali.org موقعة من سلطة شهادة أمن طبقة النقل "Transport Layer Security" (TLS) موثوق بها من قبل متصفح الضحية. نظراً لوجود سلطات الشهادات على وجه التحديد لمنع هذا النوع من المشكلات، فإنها تقدم شهادات فقط للأشخاص الذين تم التحقق من هويتهم والذين قدموا أدلة على أنهم يتحكمون في موقع الويب المقابل.

cdimage.kali.org

تشير الارتباطات الموجودة على صفحة التنزيل إلى مجال (Domain) **cdimage.kali.org**، الذي يعيد توجيهك لمرآة قريبة منك، مما يحسن سرعة النقل مع تقليل العبء على خوادم Kali المركزية.يمكن الاطلاع على قائمة بالمرايا المتوفرة هنا:
http://cdimage.kali.org/README.mirrorlist

٢.١.٢. ماذا يوجد في قسم "Downloads"

تعرض صفحة التنزيل الرسمية قائمة قصيرة من صور ISO، كما هو مبين في الشكل ١.٢. "قائمة الصور المعروضة للتنزيل".

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to **download Kali Linux** in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/.

Image Name	Download	Size	Version	sha256sum
Kali 64 bit	ISO | Torrent	2.9G	2016.2	1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601a5d454fa0431
Kali 32 bit	ISO | Torrent	2.9G	2016.2	c94772c4fd71f50b245c7b15f4f225ad7c751879f501fa1cf698beb1460c0bf5
Kali 64 bit Light	ISO | Torrent	1.1G	2016.2	997f5ed0f7c99c4518288c7e2c4b684b1bdcc2fbe02c152d7ecbd17f0536c29f
Kali 32 bit Light	ISO | Torrent	1.1G	2016.2	590e6df2e8e0b4d42bf3dd4e4c7d6acf24b7262fabda52a0c6c3b35006def295
Kali 64 bit e17	ISO | Torrent	2.7G	2016.2	404d0fd917a404cf6c894b5bd87171ebf8eb445bd5573a3e78f88629067d694b
Kali 64 bit Mate	ISO | Torrent	2.8G	2016.2	cd11b7085cc7d71546488106c2eedf85386fe73d731bedf38991661270dd91db
Kali 64 bit Xfce	ISO | Torrent	2.7G	2016.2	3e08e5420b368183606b105cf2cb1276dd024afe3e2b2e3187d7d37ec1320c41
Kali 64 bit LXDE	ISO | Torrent	2.7G	2016.2	7461882843e5a0fc37979850994fb5755249a176429f9e67805bd7f6baa5bb62
Kali armhf	Image | Torrent	0.7G	2016.2	f192289b6bc64bab7197a90627ced2477c7c98bd20c1d29f442a152e169dae42
Kali armel	Image | Torrent	0.7G	2016.2	efb6f487feab1c9141f28da22c73cbc5217325bf46298f899ac89c39c19aa5f5

شكل ١.٢. قائمة الصور المعروضة للتنزيل

تشير جميع صور الأقراص المسمى 32 أو 64 بت إلى الصور المناسبة لوحدات المعالجة المركزية، الموجودة في معظم أجهزة الحاسوب المكتبية والحاسوب المحمول الحديث. إذا كنت تقوم بالتنزيل للاستخدام على جهاز حديث إلى حد ما، فمن المحتمل أنه يحتوي على معالج 64 bit. إذا لم تكن متأكدًا، فكن على يقين من أن جميع معالجات 64 bit يمكنها تشغيل 32 bit. يمكنك دائمًا تنزيل وتشغيل صورة 32 bit. والعكس ليس صحيحًا.

إذا كنت تخطط لتثبيت Kali على جهاز مضمن أو هاتف ذكي أو Chromebook أو نقطة وصول أو أي جهاز آخر باستخدام معالج ARM، فيجب عليك استخدام Linux armel أو صور armhf.

هل معالجي 32 أو 64 بت؟

في **Windows**، يمكنك العثور على هذه المعلومات عن طريق تشغيل تطبيق "معلومات النظام" (الموجود في مجلد "البرامج الملحقة"> "أدوات النظام"). على شاشة ملخص النظام، يمكنك فحص حقل "نوع النظام": سوف يحتوي على "حاسوب يستند إلى x64" لوحدة المعالجة المركزية 64 bit أو "حاسوب يستند إلى x86" لوحدة المعالجة المركزية 32 bit.

في **OS X / macOS**، لا يوجد تطبيق قياسي يعرض هذه المعلومات ولكن لا يزال بإمكانك استنتاجها من مخرجات الأمر **uname -m** الذي يتم تشغيله على الـ terminal. سيرجع x86_64 لنظام يحتوي على نواة 64 bit (والذي لا يمكن تشغيله إلا على وحدة المعالجة المركزية 64 bit) وعلى الأنظمة التي تحتوي على نواة 32 bit، سيرجع i386 أو شيء مشابه (i486 أو i586 أو i686). يمكن تشغيل أي نواة 32 bit على وحدة المعالجة المركزية 64 bit، ولكن بما أن Apple تحكم في الأجهزة والبرامج، فمن غير المرجح أن تجد هذا التكوين.

في **Linux**، يمكنك التحقق من حقل flags في الملف الافتراضي /proc/cpuinfo. إذا كانت تحتوي على lm، فإن وحدة المعالجة المركزية لديك هي 64 bit؛ غير ذلك، يعني 32 bit. سيخبرك سطر الأوامر التالي بنوع وحدة المعالجة المركزية لديك:

```
grep -qP '^flags\s*:.*\blm\b' /proc/cpuinfo &&
echo 64-bit || echo 32-bit
64-bit
```

الآن بعد أن عرفت ما إذا كنت تحتاج إلى صورة 32 bit أو 64 bit، هناك فقط خطوة واحدة متبقية: تحديد نوع الصورة. تعد صورة Kali Linux الافتراضية و Kali Linux Light كلاهما من ISOs المباشرة التي يمكن استخدامها لتشغيل النظام المباشر أو لبدء عملية التثبيت. أنها تختلف في مجموعة التطبيقات المثبتة مسبقا. تأتي الصورة الافتراضية مع سطح مكتب Gnome ومجموعة كبيرة من الحزم التي وجد أنها مناسبة لمعظم اختبارات الاختراق، في حين تأتي الصورة الخفيفة مع سطح مكتب XFCE (الذي هو أقل طلباً على موارد النظام)، ومجموعة محدودة من الحزم، مما يسمح لك باختيار التطبيقات التي تحتاجها فقط. تستخدم الصور الأخرى بيئات سطح مكتب مختلفة ولكنها تأتي بنفس المجموعة الكبيرة الحجم مثل الصورة الرئيسية.

بمجرد أن تقرر الصورة التي تحتاجها، يمكنك تنزيل الصورة من خلال النقر على "ISO" في الصف المخصص. أو يمكنك تنزيل الصورة من شبكة BitTorrent الند للند من خلال النقر على "Torrent"، شريطة أن يكون لديك عميل BitTorrent مرتبط بامتدادtorrent..

أثناء تنزيل صورة ISO التي اخترتها، يجب أن تأخذ ملاحظة المجموع الاختباري المكتوب في عمود "sha256sum". بمجرد تنزيل صورتك، ستستخدم هذا المجموع الاختباري للتحقق من أن الصورة التي تم تنزيلها تتطابق مع الصورة التي وضعها مطورو Kali عبر الإنترنت (انظر القسم التالي).

٢.١.٣. التحقق من النزاهة والأصالة

يجب على محترفي الأمان التحقق من سلامة أدواتهم ليس فقط لحماية بياناتهم وشبكاتهم ولكن أيضًا لعملائهم. بينما تكون صفحة تنزيل Kali محمية بواسطة TLS، يشير رابط التنزيل الفعلي إلى عنوان URL غير مشفر لا يوفر أي حماية ضد هجمات man-in-the-middle المحتملة. حقيقة أن كالي تعتمد على شبكة من المرايا الخارجية لتوزيع الصورة يعني أنك يجب ألا تثق ثقة عمياء بما تقوم بتنزيله. قد تكون المرآة التي تم توجيهك إليها قد تعرضت للاختراق، أو قد تكون ضحية لهجوم بنفسك.

للتخفيف من ذلك، يوفر مشروع Kali دائمًا مقاطع اختبارية للصور التي يوزعها. ولكن لجعل هذا الفحص فعالًا، يجب أن تكون على يقين من أن المجموع الاختباري الذي استخرجته هو المجموع الاختباري الذي نشره مطورو Kali Linux. لديك طرق مختلفة للتأكد من هذا.

٢.١.٣.١. الاعتماد على موقع TLS المحمي

عندما تسترجع المجموع الاختباري من صفحة الويب للتنزيل المحمي بـ TLS، فإن أصلها مضمون بشكل غير مباشر بواسطة نموذج أمان شهادة X.509: المحتوى الذي تراه يأتي من موقع ويب يخضع فعلياً لسيطرة الشخص الذي طلب شهادة TLS.

الآن يجب عليك إنشاء المجموع الاختباري لصورتك التي تم تنزيلها والتأكد من مطابقتها لما قمت بتسجيله من موقع Kali:

```
$ sha256sum kali-linux-2016.2-amd64.iso
1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601a5d454fa0431
kali-linux-2016.2-amd64.iso
```

إذا تطابق المجموع الاختباري الذي تم إنشاؤه مع الموجود في صفحة تنزيل Kali Linux، فلديك الملف الصحيح. في حالة اختلاف النتائج، هناك مشكلة، رغم أن هذا لا يشير إلى حل وسط أو هجوم؛ التنزيلات تتلف أحيانًا لأنها تجتاز الإنترنت. جرب التنزيل مرة أخرى، من مرآة Kali الرسمية الأخرى، إن أمكن (انظر cdimage.kali.org لمزيد من المعلومات حول المرايا المتوفرة).

٢.٣.١.٢. الاعتماد على شبكة PGP الخاصة بالثقة

إذا كنت لا تثق في HTTPS للمصادقة، فعندك جنون العظمة قليلاً ولكن معك حق. هناك العديد من الأمثلة لسلطات الشهادات التي تتم إدارتها بشكل سيء والتي أصدرت شهادات فاسدة، والتي انتهى الأمر بإساءة استخدامها. قد تكون أيضًا ضحية هجوم man-in-the-middle "الودي" الذي يتم تنفيذه على العديد من شبكات الشركات، وذلك باستخدام متجر ثقة مخصص مزروع بواسطة المستعرض يقدم شهادات مزيفة لجميع مواقع الويب المشفرة SSL، مما يسمح لمراجعي الشركات بمراقبة حركة المرور المشفرة.

في حالات كهذه، نوفر أيضًا مفتاح GnuPG الذي نستخدمه للتوقيع على اختبار الصور التي نقدمها. معرّفات المفتاح والبصمات معروضة هنا:

```
pub   4096R/7D8D0BF6 2012-03-05 [expires: 2018-02-02]
Key fingerprint = 44C6 513A 8E4F B3D3 0875  F758
ED44 4FF0 7D8D 0BF6
uid  Kali Linux Repository devel@kali.org
sub   4096R/FC0D0DCB 2012-03-05 [expires: 2018-02-02]
```

هذا المفتاح جزء من شبكة ثقة عالمية لأنه تم توقيعه على الأقل من قبلي (Raphaël Hertzog) وأنا جزء من شبكة الثقة بسبب استخدامي المكثف لـ GnuPG كمطور لديبيان.

طراز الأمان PGP / GPG فريد من نوعه. يمكن لأي شخص إنشاء أي مفتاح له أي هوية، لكنك لن تثق بهذا المفتاح إلا إذا تم توقيعه بواسطة مفتاح آخر تثق به بالفعل. عندما تقوم بالتوقيع على مفتاح، فإنك تقر بأنك قابلت حامل المفتاح وأنك تعلم أن الهوية المرتبطة صحيحة. ويمكنك تحديد المجموعة الأولية من المفاتيح التي تثق بها، والتي تتضمن بوضوح مفتاحك الخاص.

هذا النموذج له حدوده الخاصة، لذا يمكنك اختيار تنزيل مفتاح Kali العام عبر HTTPS (أو من خادم مفاتيح) وقرر فقط أن تثق به لأن بصمة أصبعه تتطابق مع ما أعلناه في أماكن متعددة، بما في ذلك أعلاه فقط في هذا الكتاب:

```
$ wget -q -O - https://www.kali.org/archive-key.asc
| gpg --import

[ or ]

$ gpg --keyserver hkp://keys.gnupg.net --recv-key
7D8D0BF6

gpg: key 7D8D0BF6: public key "Kali Linux
Repository <devel@kali.org>" imported

gpg: Total number processed: 1

gpg: imported: 1  (RSA: 1)

[...]

$ gpg --fingerprint 7D8D0BF6

[...]

Key fingerprint = 44C6 513A 8E4F B3D3 0875  F758
ED44 4FF0 7D8D 0BF6

[...]
```

الآن وقد حصلنا على المفتاح، يمكننا استخدامه للتحقق من المجموع الاختباري لصور التوزيعة. لنقم بتنزيل الملف باستخدام المجموع الاختباري (SHA256SUMS) وملف التوقيع المقترن (SHA256SUMS.gpg) والتحقق من التوقيع:

```
$wget http://cdimage.kali.org/current/SHA256SUMS
[...]
$wget http://cdimage.kali.org/current/SHA256SUMS.gpg
[...]
$gpg --verify SHA256SUMS.gpg SHA256SUMS
gpg: Signature made Thu 16 Mar 2017 08:55:45 AM MDT
gpg: using RSA key ED444FF07D8D0BF6
gpg: Good signature from "Kali Linux Repository <devel@kali.org>"
```

إذا تلقيت رسالة "توقيع جيد (Good signature)"، فيمكنك الوثوق في محتوى ملف SHA256SUMS واستخدامه للتحقق من الملفات التي قمت بتنزيلها. غير ذلك، هناك مشكلة. يجب عليك مراجعة ما إذا كنت قد قمت بتنزيل الملفات من مرآة Kali Linux شرعية. (قانونية أو معتمدة)

لاحظ أنه يمكنك استخدام سطر الأوامر التالي للتحقق من أن الملف الذي تم تنزيله له نفس المجموع الاختباري المدرج في SHA256SUMS، شريطة أن يكون ملف ISO الذي تم تنزيله في نفس المجلد:

```
$ grep kali-linux-2016.2-amd64.iso SHA256SUMS | sha256sum -c
kali-linux-2016.2-amd64.iso: OK
```

إذا لم تحصل على موافقة "OK"، فالملف الذي قمت بتنزيله يختلف عن الملف الذي أصدره فريق Kali. لا يمكن الوثوق بها ويجب عدم استخدامها.

٤.١.٢. نسخ الصورة على قرص DVD-ROM أو مفتاح USB

ما لم ترغب في تشغيل Kali Linux في جهاز افتراضي، فإن صورة ISO تكون محدودة الاستخدام بحد ذاتها. يجب عليك نسخها على قرص DVD-ROM أو نسخها على مفتاح USB لتتمكن من تشغيل جهازك بنظام Kali Linux.

لن نغطي كيفية نسخ صورة ISO على قرص DVD-ROM، حيث تختلف العملية اختلافًا كبيرًا حسب النظام الأساسي والبيئة، ولكن في معظم الحالات، يؤدي النقر بزر الماوس الأيمن على ملف iso. إلى ستجد في القائمة برنامج حرق DVD- ROM. جرب!

> في هذا القسم، ستتعلم كيفية الكتابة فوق قرص باستخدام صورة Kali Linux ISO. تحقق دائمًا من فحص القرص المستهدف قبل بدء العملية، حيث من المحتمل أن يتسبب خطأ واحد في فقد البيانات بشكل كامل وقد يتسبب في تلف الإعداد (setup) الخاص بك بشكل لا يمكن إصلاحه.

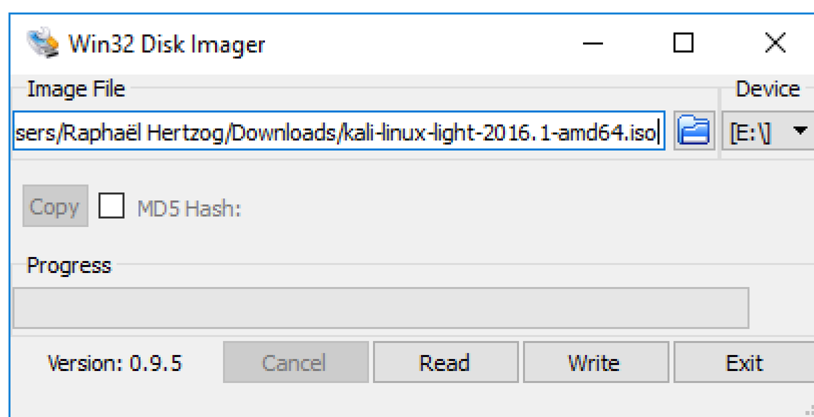
١.٤.١.٢. إنشاء محرك USB كالي قابل للتشغيل على Windows

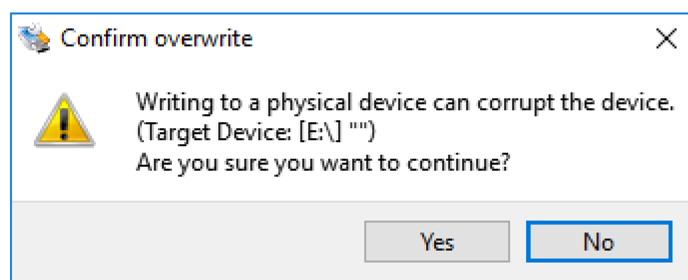
كشرط أساسي، يجب عليك تنزيل وتثبيت Win32 Disk Imager:

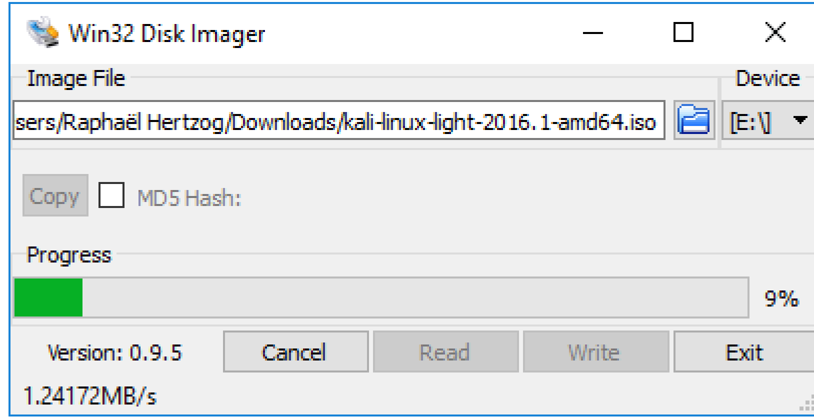
https://sourceforge.net/projects/win32diskimager/

قم بتوصيل مفتاح USB بجهاز الحاسوب الشخصي الخاص بك الذي يعمل بنظام Windows ولاحظ محدد محرك الأقراص المرتبط به (على سبيل المثال، "E:").

قم بتشغيل Win32 Disk Imager واختر ملف Kali Linux ISO الذي تريد نسخه على مفتاح USB. تحقق من أن حرف الجهاز المحدد يتوافق مع ذلك المعين لمفتاح USB. بمجرد التأكد من تحديد محرك الأقراص الصحيح، انقر فوق زر "Write" وتأكد من أنك تريد الكتابة فوق محتويات مفتاح USB كما هو موضح في "شكل 2.2. عملية الكتابة ببرنامج Win32 Disk imager".





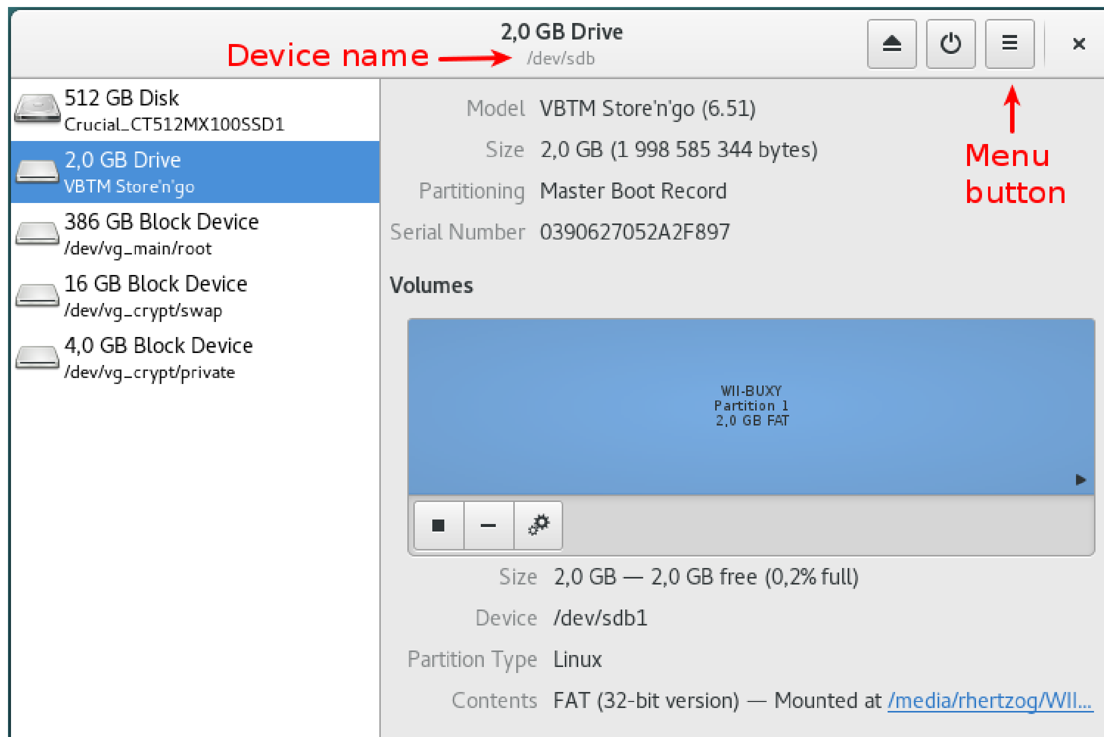


شكل 2.2. عملية الكتابة ببرنامج Win32 Disk imager

بمجرد اكتمال النسخ، أخرج محرك USB بأمان من نظام Windows. يمكنك الآن استخدام جهاز USB لتشغيل Kali Linux.

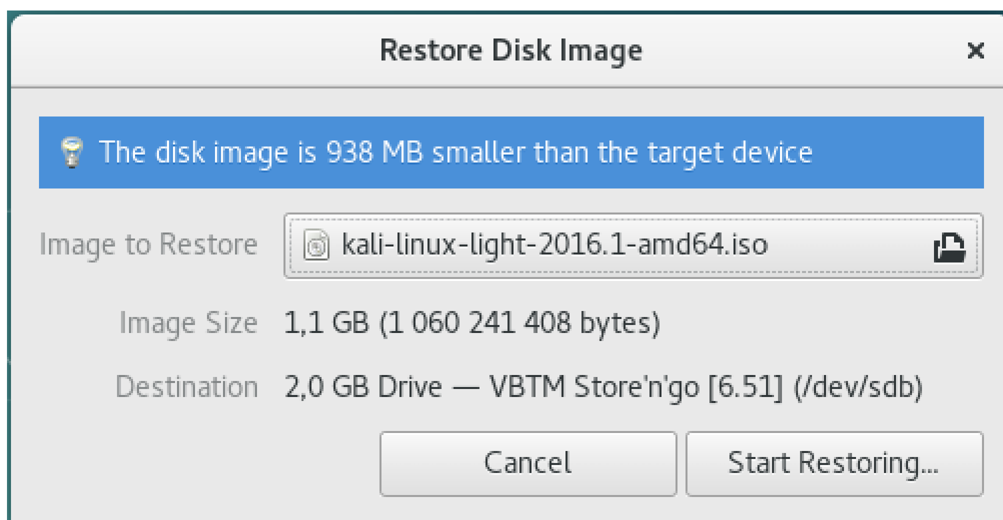
٢.٤.١.٢. إنشاء محرك أقراص USB قابل للإقلاع على نظام Linux

من السهل إنشاء مفتاح Kali Linux USB قابل للإقلاع في بيئة Linux. تأتي بيئة سطح مكتب GNOME، والتي يتم تثبيتها افتراضياً في العديد من توزيعات Linux، مع أداة (Disks utility) (في حزمة الأداة المساعدة gnome-disk-tool، والتي تم تثبيتها بالفعل في صورة Kali). يعرض هذا البرنامج قائمة بالأقراص، والتي يتم تحديثها بشكل مستمر عند توصيل قرص أو فصله. عند تحديد مفتاح USB الخاص بك في قائمة الأقراص، ستظهر معلومات مفصلة وسوف تساعدك على تأكيد تحديد القرص الصحيح. لاحظ أنه يمكنك العثور على اسم الجهاز الخاص به ((أو مسار الجهاز لأن كل شيء في لينكس عبارة عن ملفات)) في شريط العنوان كما هو موضح في الشكل ٣.٢، "GNOME Disks".



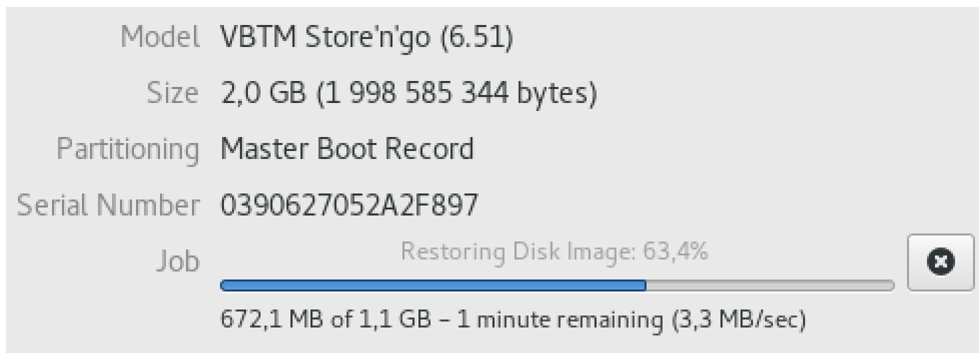
شكل ٣.٢. GNOME Disks

انقر على زر القائمة واختار ...Restore Disk Image في القائمة المنبثقة المعروضة. حدد صورة ISO التي قمت بتنزيلها مسبقًا وانقر فوق "...Start Restoring" كما هو موضح في الشكل ٤.٢. "Restore Disk Image Dialog".



شكل ٤.٢. "Restore Disk Image Dialog"

استمتع بفنجان من القهوة بينما تنتهي من نسخ الصورة على مفتاح USB شكل) 2.5 .(“Progression of the Image Restoration



شكل ٥.٢. Progression of the Image Restoration

إنشاء محرك أقراص USB قابل للإقلاع من سطر الأوامر

على الرغم من أن العملية الرسومية واضحة إلى حد ما، إلا أن العملية سهلة لمستخدمي سطر الأوامر.

عندما تقوم بإدخال مفتاح USB الخاص بك، فإن نواة Linux ستكتشفه وتعين له اسمًا، وهو مطبوع في سجلات النواة. يمكنك العثور على اسمها عن طريق فحص السجلات التي يتم إرجاعها بواسطة **dmesg**.

```
$ dmesg
[...]
[234743.896134] usb 1-1.2: new high-speed USB device number 6 using
ehci-pci
[234743.990764] usb 1-1.2: New USB device found, idVendor=08ec,
idProduct=0020
[234743.990771] usb 1-1.2: New USB device strings: Mfr=1,
Product=2, SerialNumber=3
[234743.990774] usb 1-1.2: Product: Store'n'go
[234743.990777] usb 1-1.2: Manufacturer: Verbatim
[234743.990780] usb 1-1.2: SerialNumber: 0390627052A2F897
[234743.991845] usb-storage 1-1.2:1.0: USB Mass Storage device
detected
[234743.992017] scsi host7: usb-storage 1-1.2:1.0
[234744.993818] scsi 7:0:0:0: Direct-Access     VBTM     Store'n'go
6.51 PQ: 0 ANSI: 0 CCS
[234744.994425] sd 7:0:0:0: Attached scsi generic sg1 type 0
[234744.995753] sd 7:0:0:0: [sdb] 3903487 512-byte logical blocks:
(2.00 GB/1.86 GiB)
[234744.996663] sd 7:0:0:0: [sdb] Write Protect is off
[234744.996669] sd 7:0:0:0: [sdb] Mode Sense: 45 00 00 08
```

```
[234744.997518] sd 7:0:0:0: [sdb] No Caching mode page found
[234744.997524] sd 7:0:0:0: [sdb] Assuming drive cache: write through
[234745.009375] sdb: sdb1
[234745.015113] sd 7:0:0:0: [sdb] Attached SCSI removable disk
```

الآن بعد أن عرفت أن مسار مفتاح USB هو dev/sdb/، يمكنك المتابعة لنسخ الصورة باستخدام الأمر **dd**:

```
#dd if=kali-linux-light-2016.2-amd64.iso of=/dev/sdb
2070784+0 records in
2070784+0 records out
1060241408 bytes (1.1 GB, 1011 MiB) copied, 334.175 s, 3.2 MB/s
```

لاحظ أنك بحاجة إلى أذونات الجذر لإتمام هذه العملية ويجب عليك أيضًا التأكد من عدم استخدام مفتاح USB. وهذا هو، يجب عليك التأكد من أنه لا يوجد أي جزء منه موصول. يفترض الأمر أيضًا أنه يتم تشغيله أثناء وجوده في المجلد الذي فيه صورة ISO، وإلا فسيتعين توفير المسار الكامل.

للعلم: **if** تعني "ملف الإدخال" و **of** "ملف الإخراج". يقوم الأمر **dd** بقراءة البيانات من ملف الإدخال وإعادة كتابتها مرة أخرى إلى ملف الإخراج. لا يُظهر أي معلومات تَقَدُّم، لذا يجب عليك التحلي بالصبر أثناء قيامه بعمله (ليس من غير المعتاد أن يستغرق الأمر أكثر من نصف ساعة!). انظر إلى مصباح نشاط الكتابة على مفتاح USB إذا كنت ترغب في التحقق من أن الأمر يعمل. يتم عرض الإحصاءات المبينة أعلاه فقط عند اكتمال الأمر.

على **OS X / macOS**، يمكنك أيضًا الضغط على CTRL + T أثناء العملية للحصول على معلومات إحصائية عن النسخة بما في ذلك كمية البيانات التي تم نسخها.

٣.٤.١.٢. إنشاء محرك أقراص USB قابل للإقلاع من OS X/mac OS

يعتمد نظام OS X/macOS على نظام UNIX، لذا فإن عملية إنشاء محرك أقراص Kali Linux USB قابل للإقلاع تشبه إجراء Linux. بمجرد قيامك بتنزيل والتحقق من ملف Kali ISO الذي اخترته، استخدم أمر **dd** لنسخه على مفتاح USB.

لتحديد اسم جهاز مفتاح USB، قم بتشغيل قائمة **diskutil** لسرد الأقراص المتوفرة على نظامك. بعد ذلك، أدخل مفتاح USB وقم بتشغيل أمر قائمة **diskutil** مرة أخرى. يجب أن يكون ثاني نتيجة للقرص الإضافي. يمكنك تحديد اسم الجهاز لمفتاح USB عن طريق مقارنة الإخراج من كلا الأمرين. ابحث عن سطر جديد يحدد قرص USB ولاحظ dev/diskX/ حيث يمثل X معرف القرص.

يجب عليك التأكد من عدم وصل مفتاح USB، والذي يمكن تنفيذه باستخدام أمر **unmount** (بافتراض أن dev/disk6/ هو اسم جهاز مفتاح USB):

```
$ diskutil unmount /dev/disk6
```

الآن انتقل إلى تنفيذ الأمر **dd**. هذه المرة، نضيف معلمة تكميلية **bs-** لحجم الكتلة. يحدد حجم الكتلة التي تتم قراءتها من ملف الإدخال ثم يتم كتابتها إلى ملف الإخراج.

```
# dd if=kali-linux-light-2016.2-amd64.iso of=/dev/disk6 bs=1M
1011+0 records in
1011+0 records out
1060241408 bytes transferred in 327.061 secs (3242328 bytes/sec)
```

هذا هو. مفتاح USB جاهز الآن ويمكنك الإقلاع منه أو استخدامه لتثبيت Kali Linux.

إنشاء محرك أقراص USB قابل للإقلاع من سطر الأوامر

للإقلاع من محرك أقراص بديل على نظام OS X / macOS، بعد تشغيل الجهاز مباشرة اضغط مع الإستمرار على مفتاح option ثم حدد محرك الأقراص الذي تريد الإقلاع منه.

٢.٢. إقلاع نظام كالي في الوضع المباشر

١.٢.٢. على حاسوب حقيقي

كشرط أساسي، تحتاج إما إلى إعداد مفتاح USB (كما هو مفصل في القسم السابق) أو قرص DVD-ROM تم حرقه كصورة Kali Linux ISO.

BIOS / UEFI مسؤول عن عملية الإقلاع المبكر ويمكن تهيئته من خلال برنامج يسمى "Setup". على وجه الخصوص، يسمح للمستخدمين باختيار جهاز الإقلاع المفضل. في حالتنا، نريد تحديد محرك أقراص DVD-ROM أو محرك أقراص USB، اعتماداً على الجهاز الذي قمت بإنشائه.

يتضمن بدء الإعداد عادةً الضغط على مفتاح معين في وقت قريب جدًا بعد تشغيل الحاسوب. غالبًا ما يكون هذا المفتاح هو Del أو Esc، وأحيانًا F2 أو F10. في معظم الأوقات، يبقى وقت الاختيار لفترة قصيرة على الشاشة عندما يشتغل الحاسوب، قبل تحميل نظام التشغيل.

بمجرد تهيئة BIOS/UEFI بشكل صحيح للإقلاع من جهازك، فإن تشغيل Kali Linux هو مجرد إدخال قرص DVD-ROM أو توصيله في محرك USB وتشغيله على الحاسوب.

تعطيل الإقلاع الآمن

Disable Secure Boot

> بينما يمكن تشغيل صور Kali Linux في وضع UEFI، إلا أنها لا تدعم الإقلاع الآمن. يجب عليك تعطيل هذه الميزة في الإعداد.

٢.٢.٢. على جهاز افتراضي

الأجهزة الافتراضية لها فوائد متعددة لمستخدمي Kali Linux. إنها مفيدة بشكل خاص إذا كنت ترغب في تجربة Kali Linux ولكنك غير مستعد للالتزام بتثبيته بشكل دائم على جهازك أو إذا كان لديك حاسوب قوي وتريد تشغيل أنظمة متعددة في وقت واحد. يعد هذا اختيارًا شائعًا للعديد من مختبري الاختراق ومتخصصي الأمان الذين يحتاجون إلى استخدام مجموعة واسعة من الأدوات المتوفرة في Kali Linux ولكن لا يزالون يريدون البقاء في نظام التشغيل الأساسي الخاص بهم. هذا يوفر لهم أيضًا القدرة على أرشفة الجهاز الافتراضي أو حذفه بشكل آمن وأي بيانات عميل قد يحتوي عليها بدلاً من إعادة تثبيت نظام التشغيل بالكامل.

تجعل ميزة اللقطة (Snap) الخاصة ببرامج المحاكاة الافتراضية من السهل تجربة العمليات التي قد تكون خطرة، مثل تحليل البرامج الضارة، مع إتاحة طريقة سهلة عن طريق استعادة اللقطة السابقة.

هناك العديد من أدوات المحاكاة الافتراضية المتاحة لجميع أنظمة التشغيل الرئيسية، بما في ذلك VirtualBox® و VMware Workstation® و Xen و KVM و Hyper-V على سبيل المثال لا الحصر. في النهاية، استخدم البرنامج الذي يناسبك، لكننا سنغطي اثنين الأكثر استخدامًا في مجال سطح المكتب: VirtualBox® و VMware Workstation Pro®، وكلاهما يعمل على Windows 10. إذا لم يكن لديك قيود سياسة الشركة أو التفضيل الشخصي، توصيتنا هي أن تجرب VirtualBox أولاً، لأنها مجانية، وتعمل بشكل جيد، (غالبًا) مفتوحة المصدر، ومتاحة لمعظم أنظمة التشغيل. بالنسبة إلى الفصول التالية، سنفترض أنك قمت بالفعل بتثبيت أداة المحاكاة الافتراضية المناسبة وأنك على علم بطريقة تشغيلها.

١.٢.٢.٢. ملاحظات مهمة

للاستفادة الكاملة من المحاكاة الافتراضية، يجب أن يكون لديك معالج بالميزات الافتراضية المناسبة ويجب ألا يتم تعطيلها بواسطة BIOS / UEFI. تحقق مرة أخرى من خيارات "**تقنية المحاكاة الافتراضية من ®Intel**" و / أو "**ميزة Intel® VT-d**" في شاشة الإعداد.

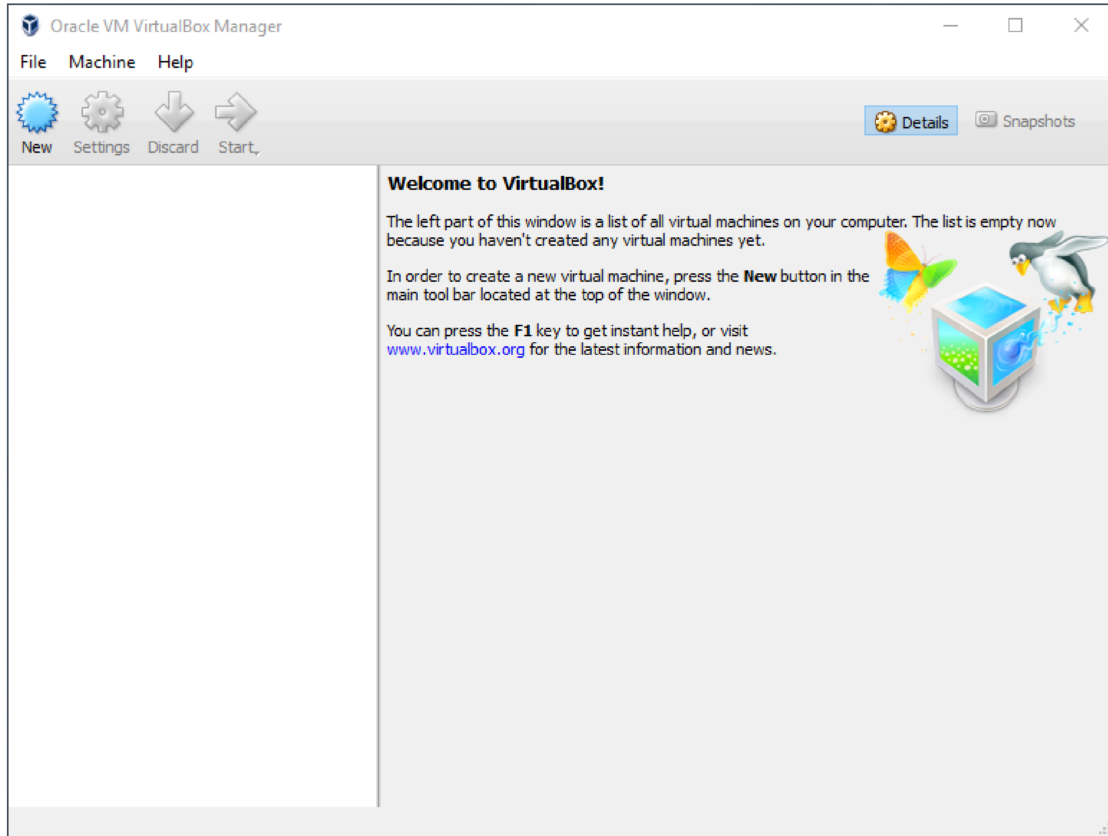
يجب أن يكون لديك أيضًا نظام تشغيل 64 bit، مثل بنية amd64 لتوزيعات Linux المستندة على Debain، وبنية x86_64 لتوزيعات Linux المستندة على RedHat، و 64-bit لنظام Windows.

إذا كنت تفتقر إلى أي من المتطلبات الأساسية، فلن تعمل أداة المحاكاة الافتراضية بشكل صحيح أو ستقتصر على تشغيل أنظمة تشغيل 32 bit فقط.

نظرًا لأن أدوات المحاكاة الافتراضية ترتبط بنظام التشغيل والأجهزة المضيفة بمستوى منخفض، فغالبًا ما يكون هناك عدم توافق بينهما. لا تتوقع أن تعمل هذه الأدوات جيدًا في نفس الوقت. احذر أيضًا من أن الإصدارات الاحترافية من Windows تأتي مع تثبيت Hyper-V وتمكينه، مما قد يتداخل مع الأداة الافتراضية التي تختارها. لإيقاف تشغيله، قم بتنفيذ "تشغيل ميزات Windows أو إيقاف تشغيلها" من إعدادات Windows.

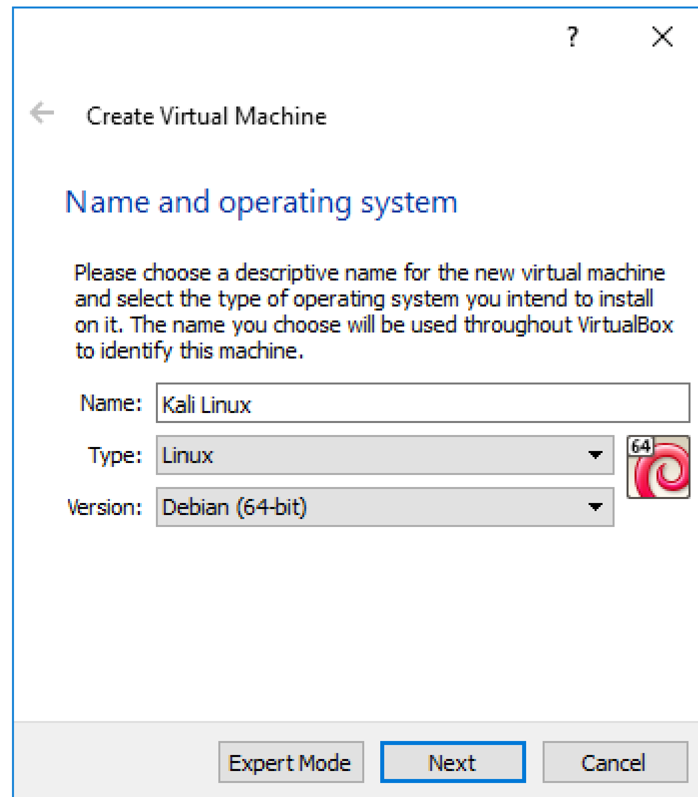
٢.٢.٢.٢. VirtualBox

تبدو الشاشة الرئيسية لـ VirtualBox مثل الشكل ٦.٢، "شاشة بدء VirtualBox".



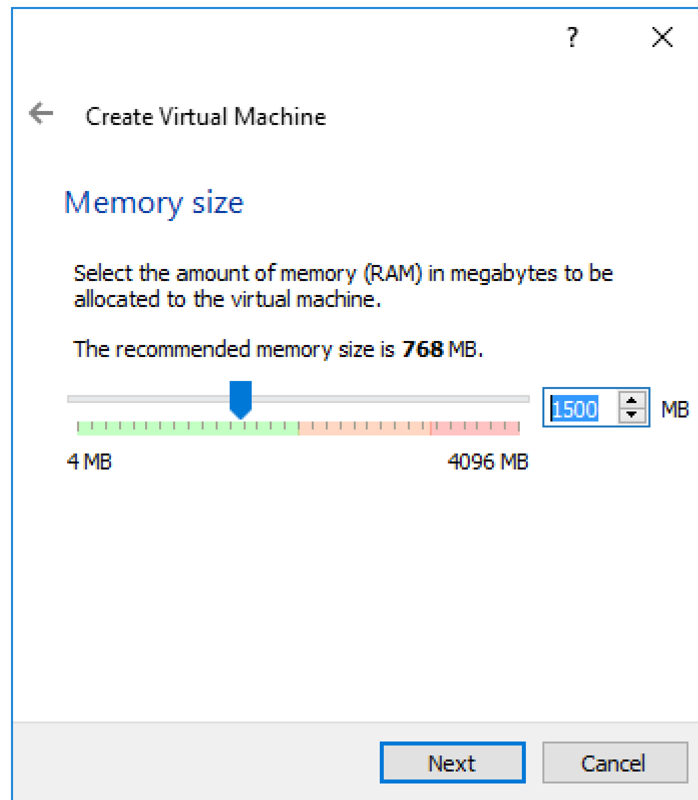
شكل ٦.٢ شاشة بدء VirtualBox

انقر فوق جديد "New" (الشكل ٧.٢ "الاسم ونظام التشغيل") لبدء معالج يرشدك خلال الخطوات المتعددة اللازمة لإدخال جميع معلمات للجهاز الافتراضي الجديد.



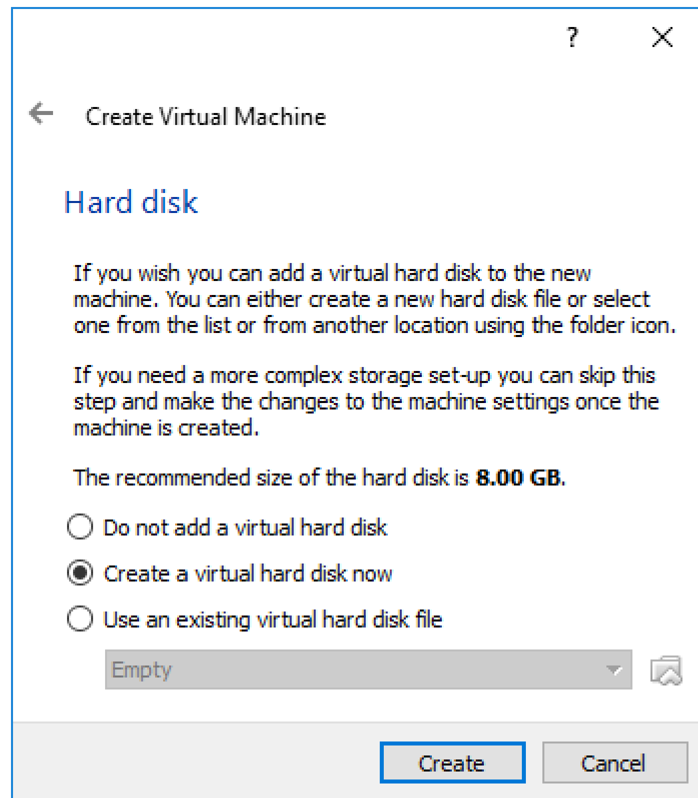
شكل ٧.٢ الاسم ونظام التشغيل

في الخطوة الأولى، الموضحة في الشكل ٧.٢ "الاسم ونظام التشغيل"، يجب تعيين اسم لجهازك الافتراضي الجديد. سوف نستخدم "Kali Linux". يجب أيضًا الإشارة إلى نوع نظام التشغيل الذي سيتم استخدامه. نظرًا لأن Kali Linux يستند إلى Debian GNU / Linux، فحدد Linux للنوع وDebian (32-bit) أو Debian (64-bit) للإصدار. على الرغم من أن أي إصدار Linux آخر سيعمل على الأرجح، فإن هذا سيساعد على التمييز بين الأجهزة الافتراضية المختلفة التي ربما تكون قد قمت بتثبيتها.



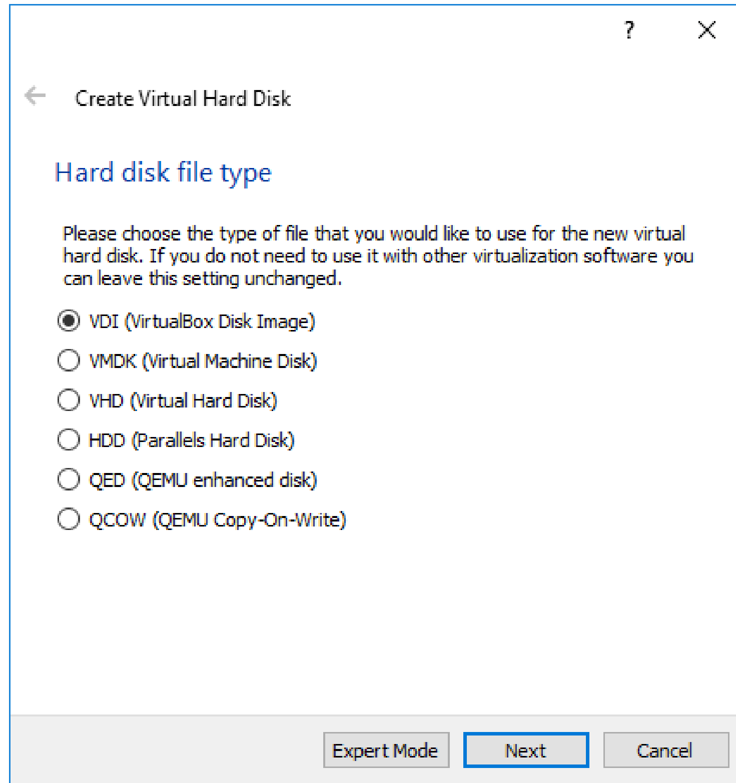
شكل ٨.٢ حجم الذاكرة

في الخطوة الثانية، يجب أن تقرر مقدار الذاكرة المخصصة للجهاز الافتراضي. على الرغم من أن الحجم الموصى به هو 768 MB مقبول لجهاز ديبيان الافتراضي الذي يعمل كخادم، فمن المؤكد أنه لا يكفي تشغيل نظام Kali لسطح المكتب، لا سيما لنظام Kali Linux المباشر لأن النظام المباشر يستخدم الذاكرة لتخزين التغييرات التي تم إجراؤها على نظام الملفات. لقد قمنا بزيادة القيمة إلى 1500 MB (الشكل ٨.٢ "حجم الذاكرة") ونوصي بشدة بتخصيص ما لا يقل عن 2048 MB من ذاكرة الوصول العشوائي (RAM).



شكل ٩.٢. القرص الصلب

في الخطوة الثالثة (الموضحة في الشكل ٩.٢، "القرص الصلب")، تتم مطالبتك باختيار قرص ثابت حقيقى أو افتراضي لجهازك الافتراضي الجديد. على الرغم من أن القرص الصلب ليس مطلوباً لتشغيل Kali Linux كنظام مباشر، إلا أننا سنضيف واحداً حتى نتمكن من عرض إجراء التثبيت لاحقًا في الفصل الرابع، تثبيت Kali Linux.



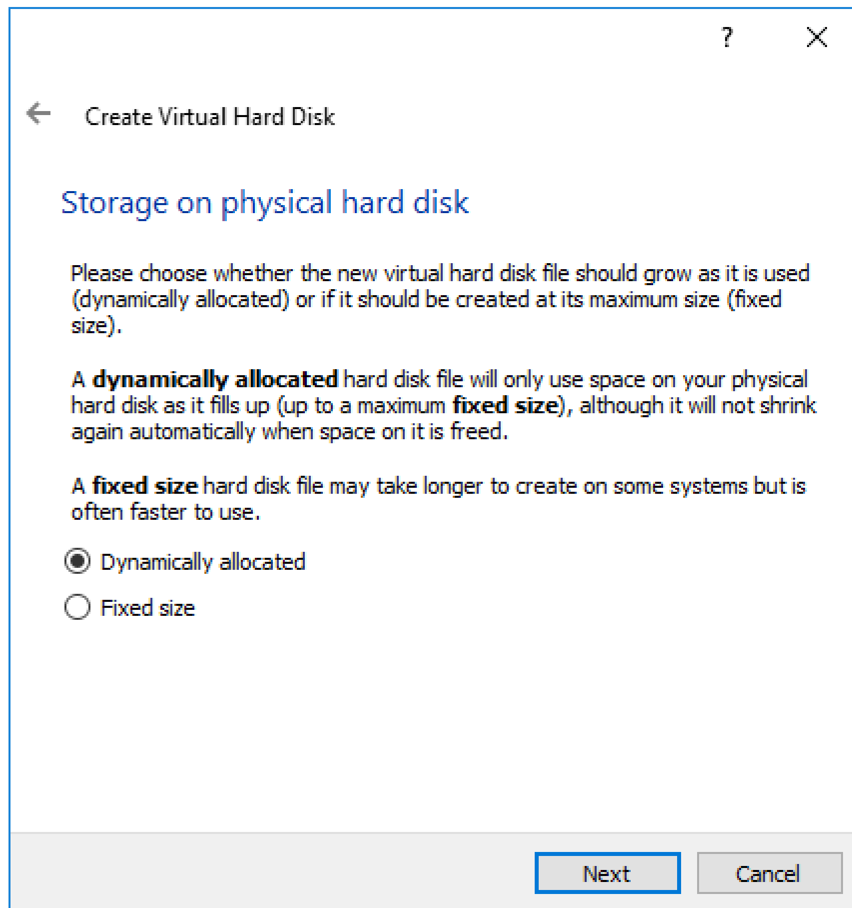
شكل ٢.١٠. نوع ملف القرص الصلب

يتم تخزين محتوى القرص الصلب للجهاز الافتراضي على الجهاز المضيف كملف.

يمكن لـ VirtualBox تخزين محتويات القرص الصلب باستخدام تنسيقات متعددة (كما هو موضح في الشكل ٢.١٠، "نوع ملف القرص الصلب"):

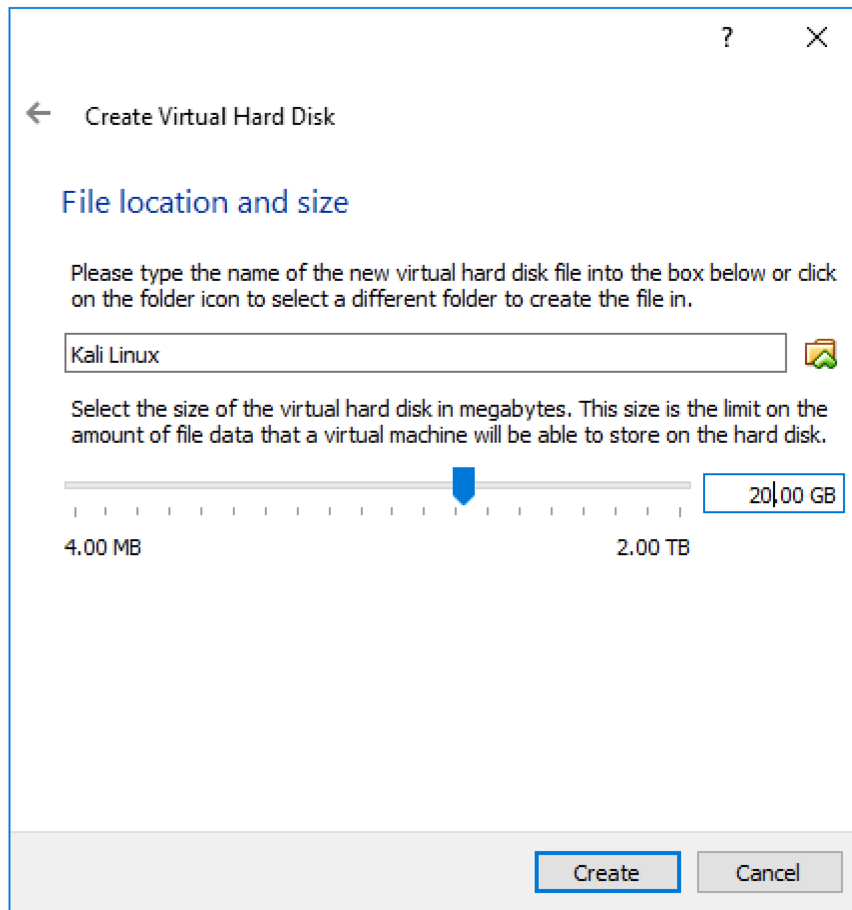
- ❖ يتوافق الإعداد الافتراضي (**VDI**) مع التنسيق الأصلي لـ VirtualBox.
- ❖ **VMDK** هو التنسيق المستخدم بواسطة VMware.
- ❖ **QCOW** هو التنسيق المستخدم بواسطة QEMU.

نحتفظ بالقيمة الافتراضية، لأنه ليس لدينا أي سبب لتغييرها. تعد القدرة على استخدام تنسيقات متعددة مثيرة للاهتمام بشكل أساسي عندما تريد نقل جهاز افتراضي من أداة افتراضية إلى أخرى.



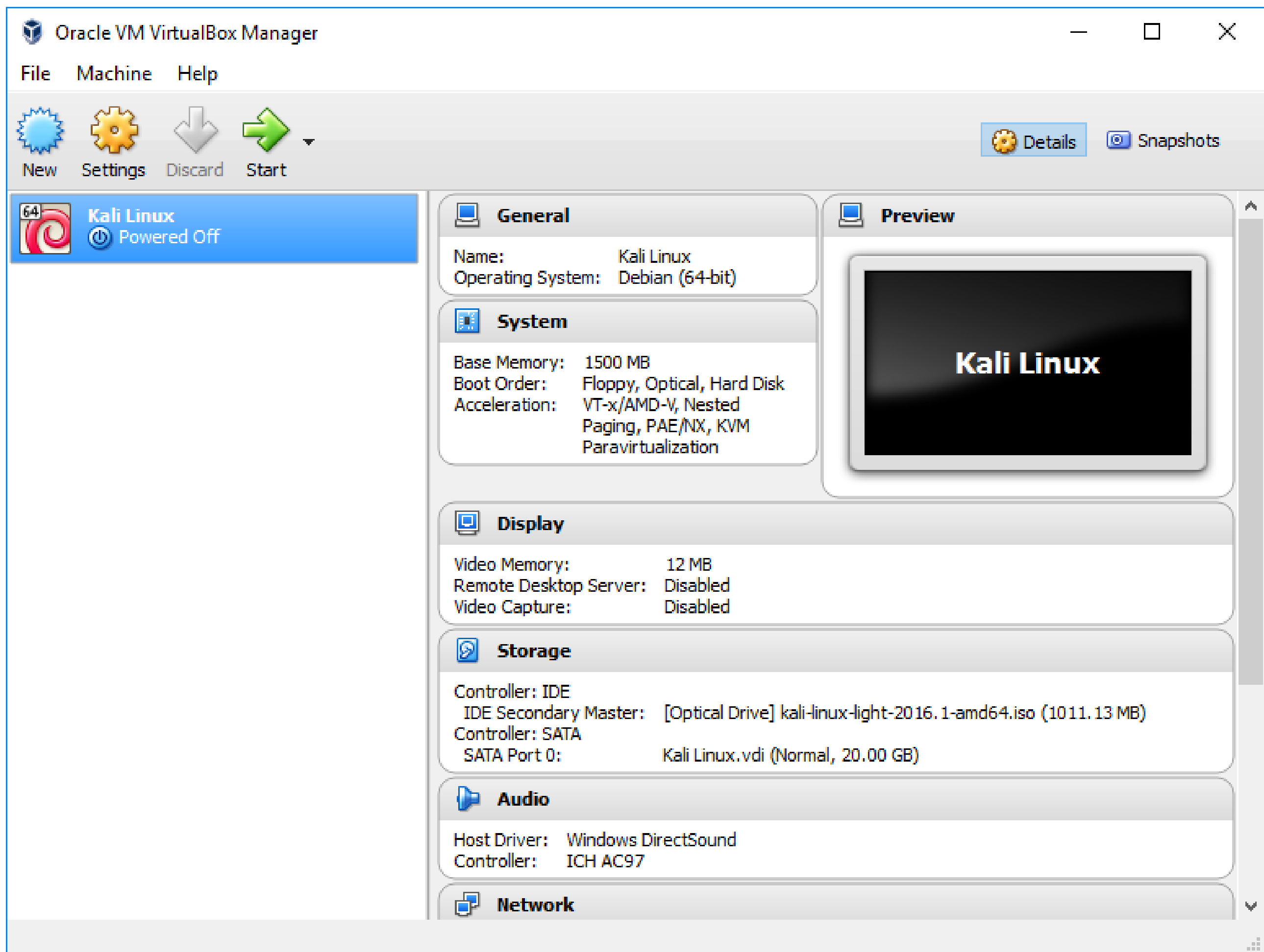
شكل ١١.٢. التخزين على القرص الصلب

يشرح نص التوضيح في الشكل ١١.٢، "التخزين على القرص الصلب" مزايا وعيوب تخصيص القرص الحيوي والثابت. نحن نقبل التحديد الافتراضي (المخصص) بشكل حيوي ("Dynamically")؛ نظراً لأننا نستخدم حاسوب محمول به أقراص SSD. في حالتنا، لا نريد تضييع المساحة ولن نحتاج إلى أداء إضافي نظراً لأن أجهزتنا سريعة جدًا بالفعل.



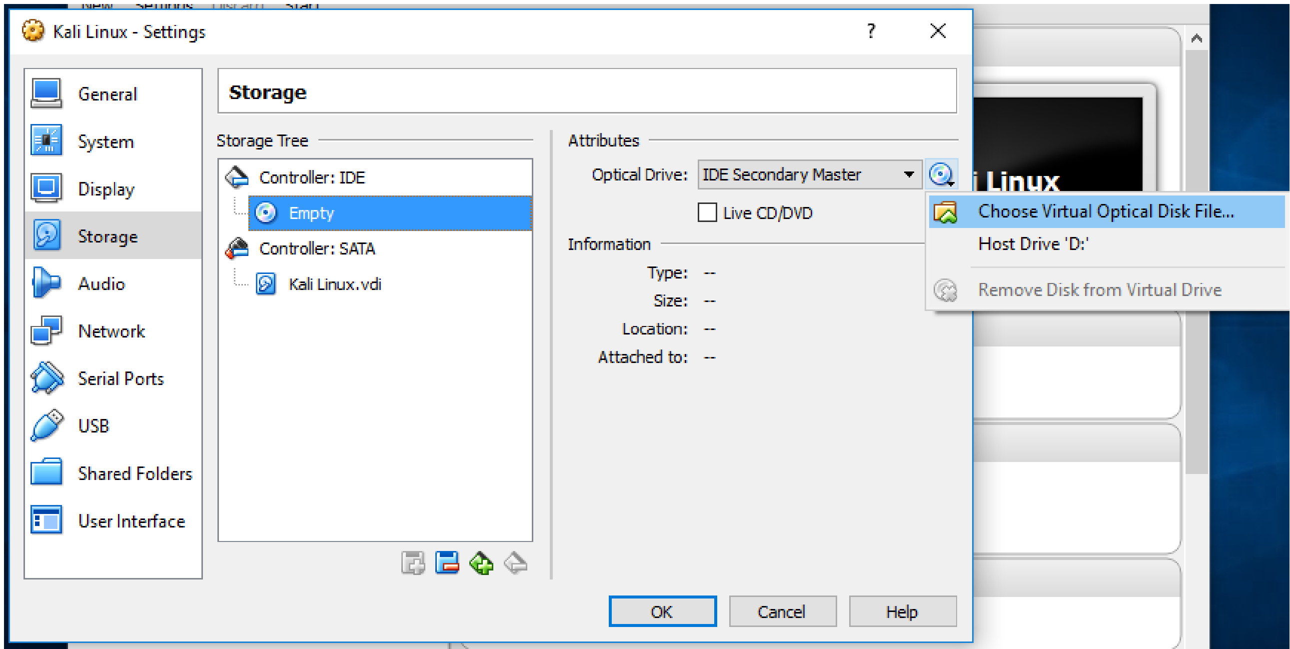
شكل ١٢.٢. موقع الملف وحجمه

لا يكفي حجم القرص الصلب الافتراضي وهو 8 GB الموضح في الشكل ١٢.٢. "موقع الملف وحجمه" للتثبيت القياسي لنظام Kali Linux، وبالتالي نزيد الحجم إلى 20 GB. يمكنك أيضًا تعديل اسم وموقع صورة القرص. يمكن أن يكون ذلك مفيدًا عندما لا يكون لديك مساحة كافية على القرص الصلب، مما يسمح لك بتخزين صورة القرص على محركات أقراص خارجية.



شكل ١٣.٢. يظهر الجهاز الافتراضي الجديد في القائمة

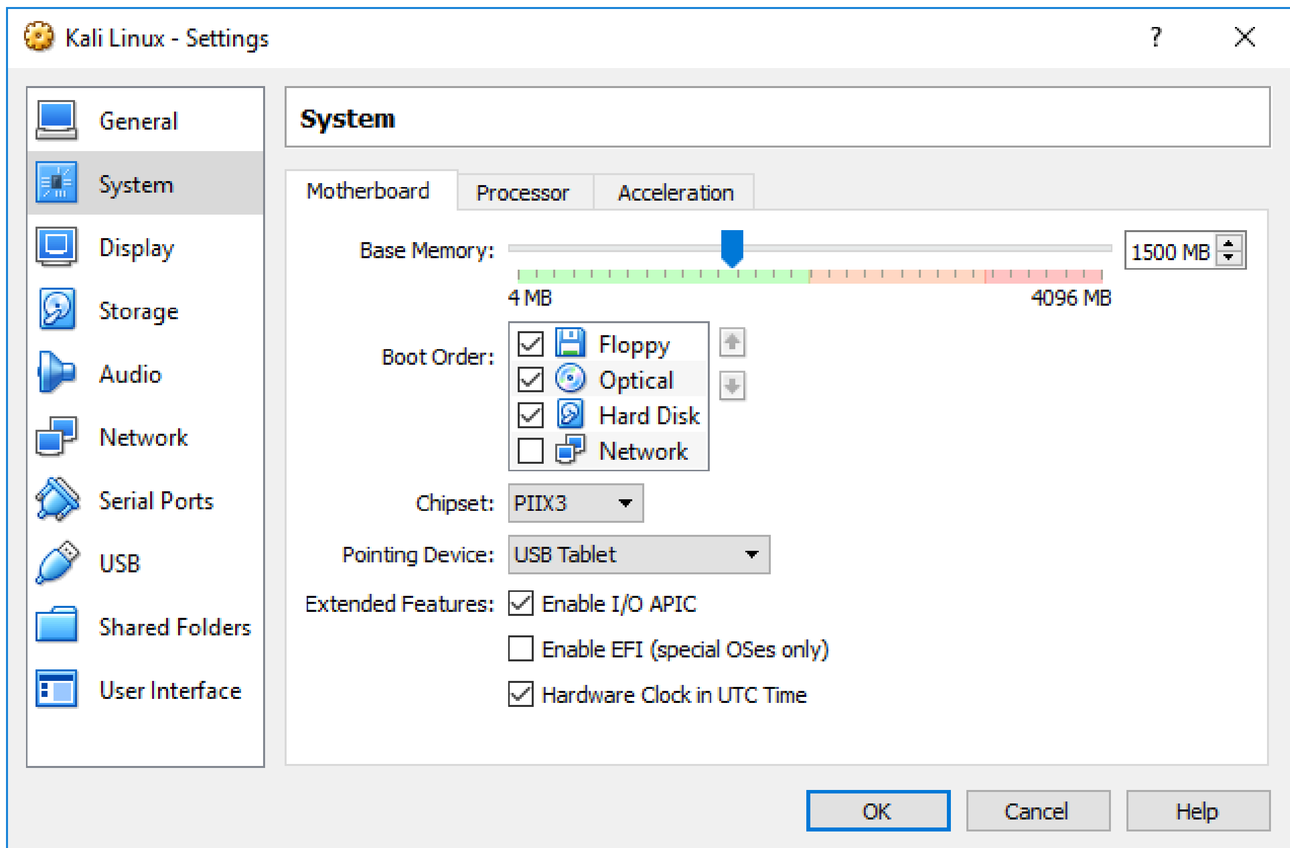
تم إنشاء الجهاز الافتراضي ولكن لا يمكننا تشغيله الان، لأنه لا يوجد نظام تشغيل مثبت. لدينا أيضا بعض الإعدادات للقرص. انقر فوق "الإعدادات (Settings)" على شاشة VM Manager ودعونا نراجع بعض الإعدادات الأكثر فائدة.



شكل ١٤.٢، إعدادات التخزين

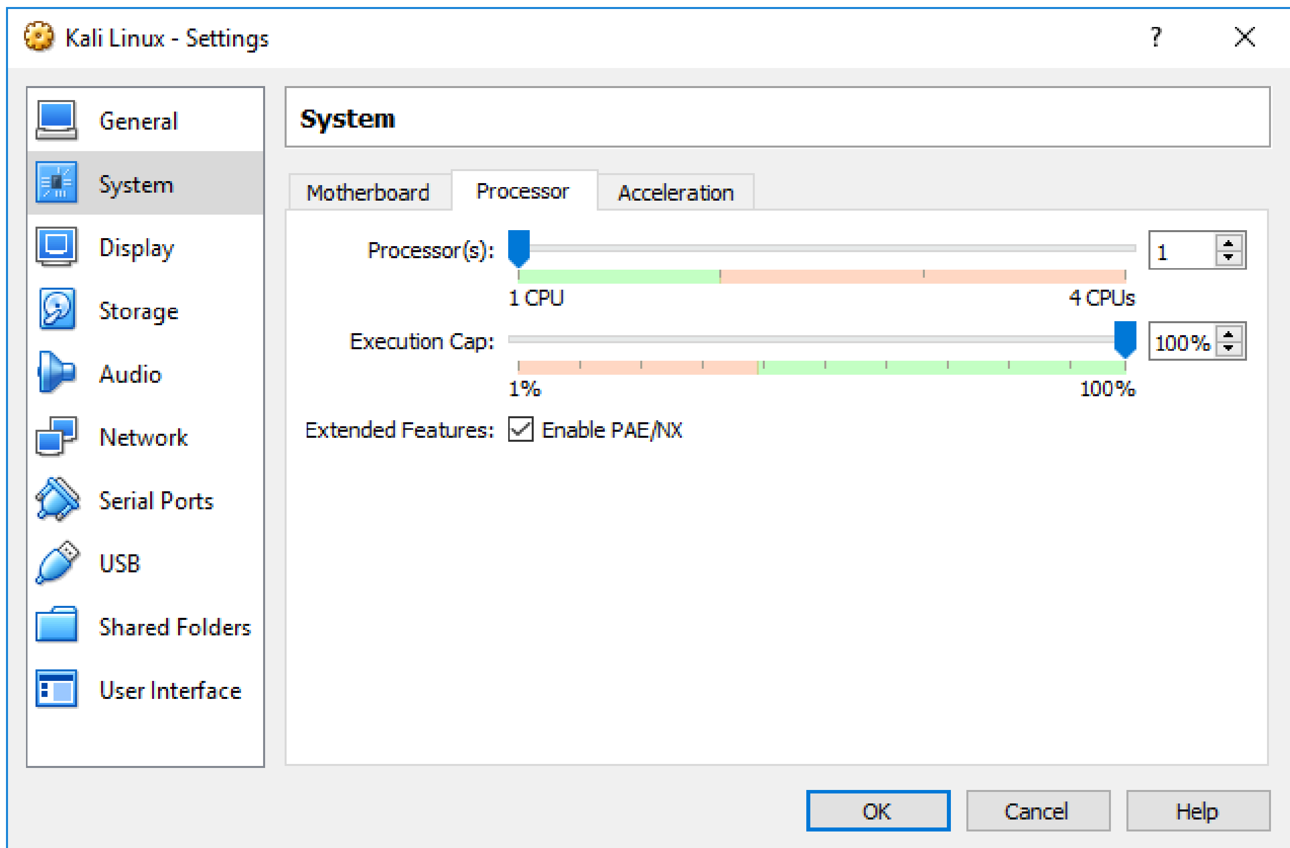
في شاشة التخزين (الشكل ١٤.٢، "إعدادات التخزين")، يجب عليك ربط صورة Kali Linux ISO بقارئ CD / DVD-ROM الافتراضي.

أولاً: حدد محرك الأقراص المضغوطة في قائمة "Storage Tree"، ثم انقر فوق أيقونة الأقراص المضغوطة الصغيرة على اليمين لعرض قائمة متفرعة حيث يمكنك "اختيار ملف القرص الظاهري ... (Choose Virtual Optical Disk File...)".



شكل ١٥.٢ إعدادات النظام: لوحة الأم

في شاشة النظام (الشكل ١٥.٢، "إعدادات النظام: لوحة الأم")، ستجد علامة تبويب "اللوحة الأم". تأكد من أن ترتيب الإقلاع يشير إلى أن النظام سيحاول أولاً الإقلاع من أي جهاز اختياري قبل تجربة القرص الثابت. في هذا التبويب يمكنك تغيير مقدار الذاكرة المخصصة للجهاز الافتراضي أيضا، إذا دعت الحاجة.

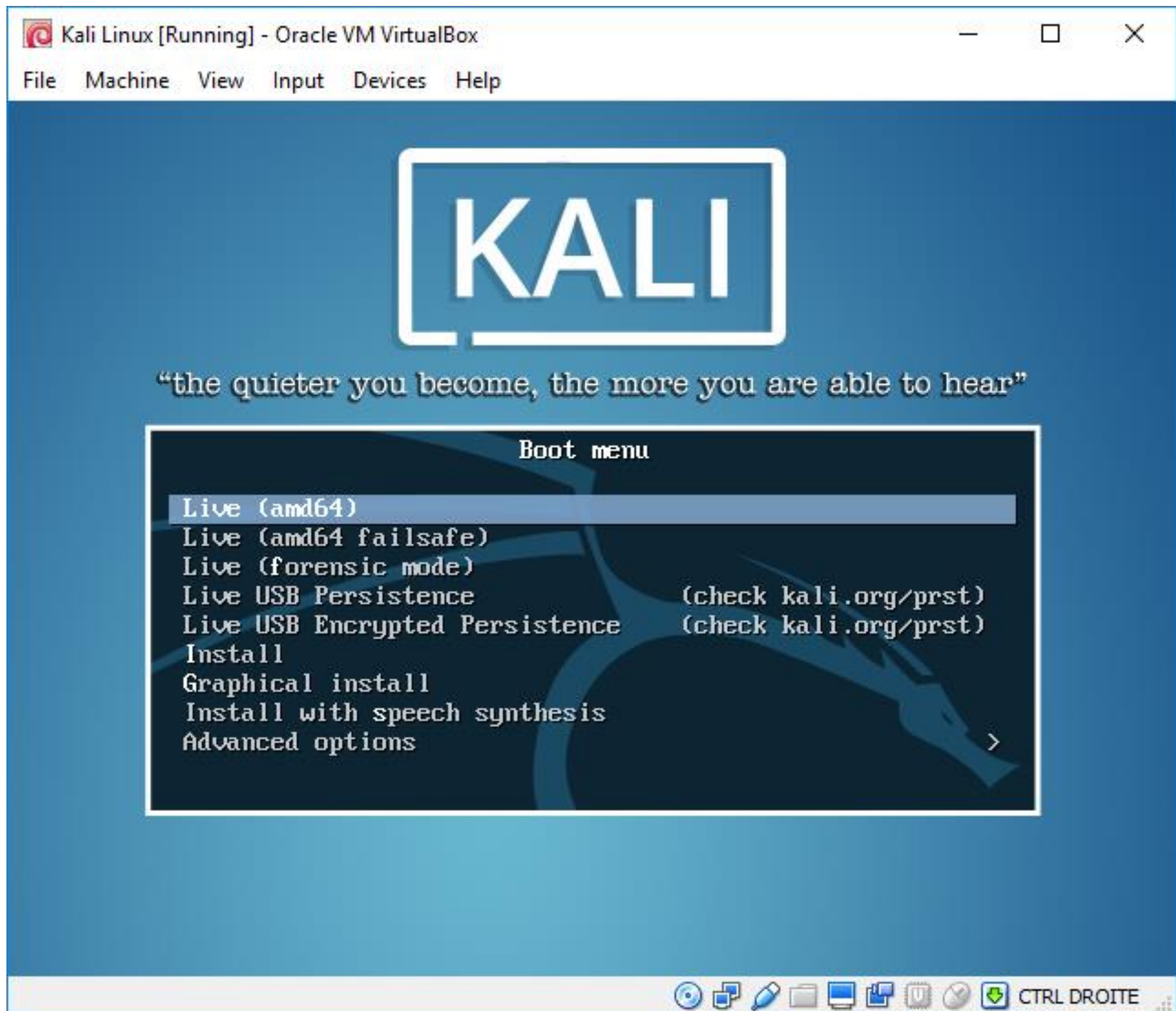


شكل ٢.١٦. إعدادات النظام: المعالج

في نفس الشاشة ولكن ضمن علامة تبويب "المعالج" (الشكل ٢.١٦، "إعدادات النظام: المعالج")، يمكنك ضبط عدد المعالجات المخصصة للجهاز الافتراضي. الأهم من ذلك، إذا كنت تستخدم صورة ذات 32 bit، فلن يتم تمكين PAE / NX أو لن يتم تشغيل صورة Kali نظراً لأن متغير (النواة) kernel الافتراضي الذي تستخدمه Kali لـ i386 (يُسمى بشكل مناسب "pae-686") يتم تجميعه بطريقة تتطلب امتداد عنوان مادي (Physical Address Extension) (PAE) في وحدة المعالجة المركزية.

هناك العديد من المعلمات الأخرى التي يمكن تهيئتها، مثل إعداد الشبكة (تحديد كيفية التعامل مع حركة المرور على بطاقة الشبكة)، ولكن التغييرات المذكورة أعلاه كافية لتتمكن من تشغيل نظام مباشر يعمل بنظام Kali Linux.

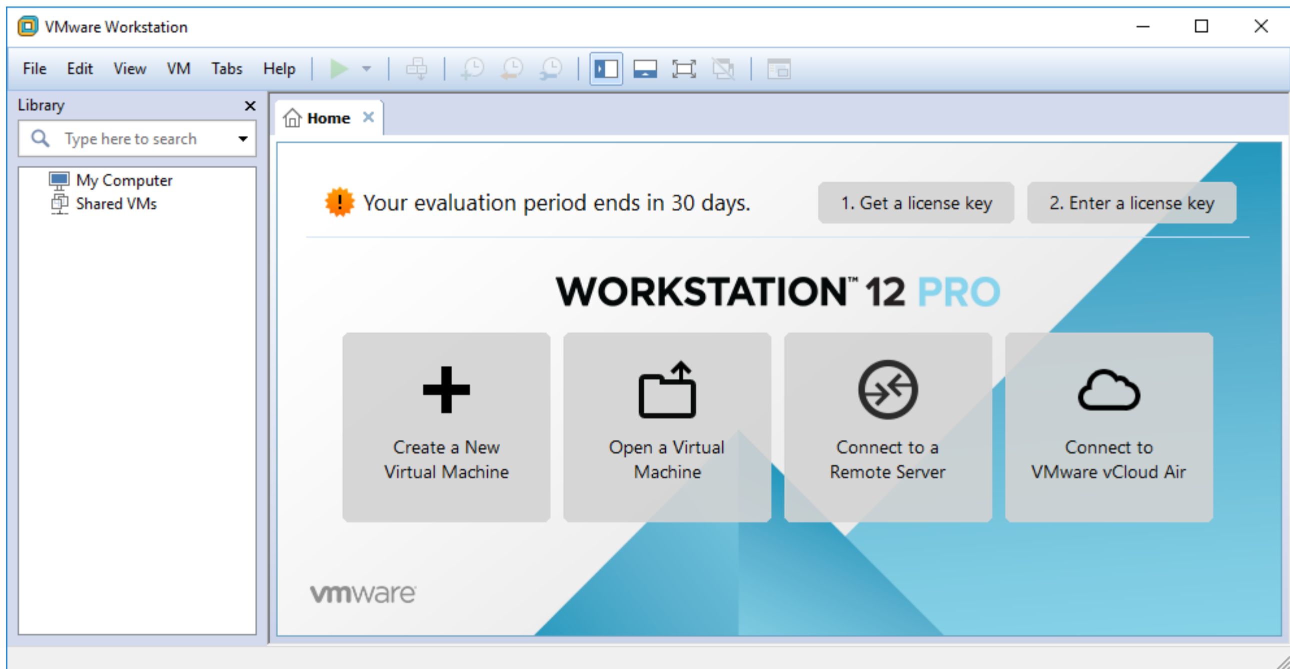
أخيرًا، انقر فوق **Boot** (إقلاع)، يجب على VM الإقلاع بشكل صحيح، كما هو موضح في الشكل ١٧.٢، "شاشة إقلاع كالي لينكس في VirtualBox". إذا لم يكن كذلك، فراجع جميع الإعدادات بعناية وحاول مرة أخرى.



شكل ١٧.٢ شاشة إقلاع كالي لينكس في VirtualBox

٢.٢.٢.٣. VMware

يشبه VirtualBox من حيث الميزات وواجهة المستخدم، لأن كلاهما صُمم خصيصا للاستخدام في أنظمة سطح المكتب، ولكن الإعدادات لجهاز افتراضي جديد مختلفة قليلاً.



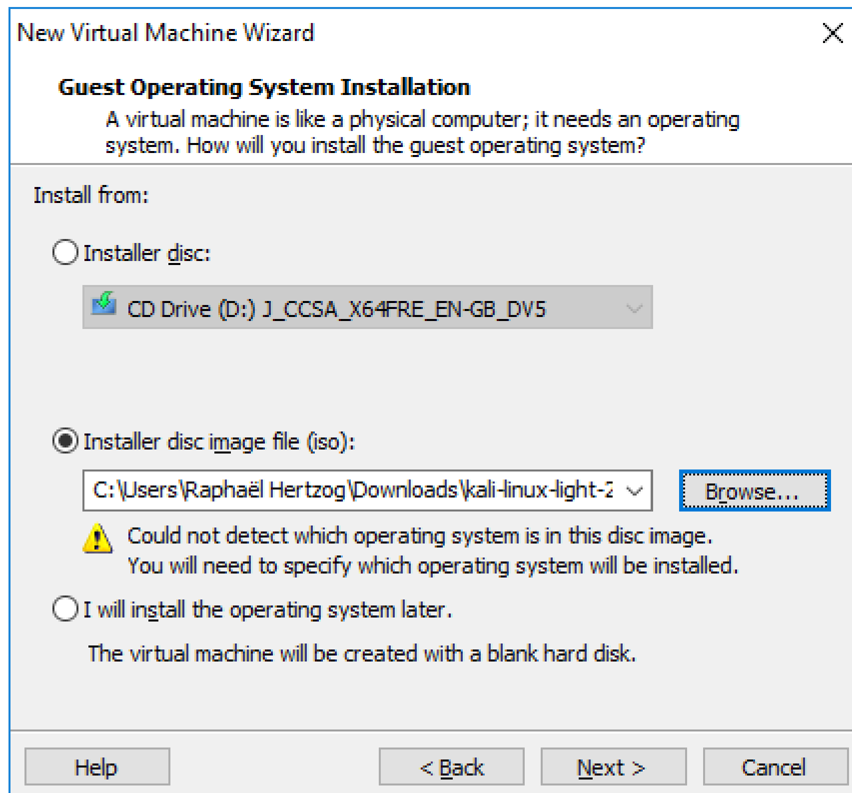
شكل ٢.١٨. شاشة بدء VMware

تعرض شاشة البداية، الموضحة في الشكل ٢.١٨، "شاشة بدء VMware"، زر إنشاء جهاز افتراضي جديد كبير (Create a New Virtual Machine) يقوم بتشغيل معالج لإرشادك خلال إنشاء جهازك الافتراضي.



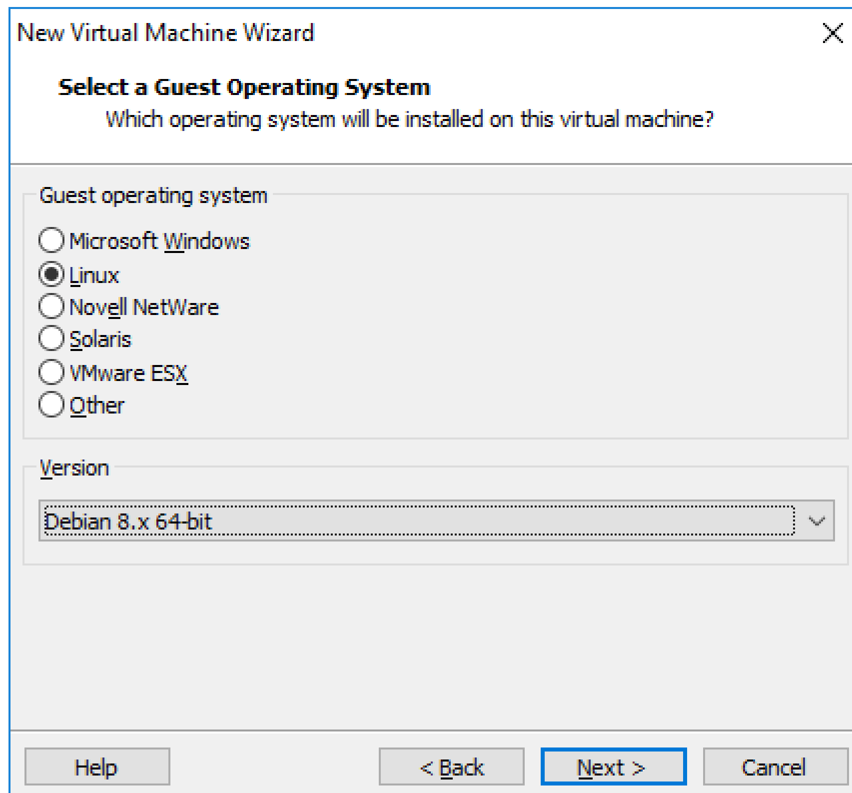
شكل ١٩.٢ معالج الجهاز الافتراضي الجديد

في الخطوة الأولى، يجب أن تقرر ما إذا كنت تريد تقديم الإعدادات المتقدمة أثناء عملية الإعداد أم لا. ليس لدينا أي متطلبات خاصة لذلك اخترنا تثبيتًا نموذجيًا (typical installation) كما هو موضح في الشكل ١٩.٢، "معالج الجهاز الافتراضي الجديد".



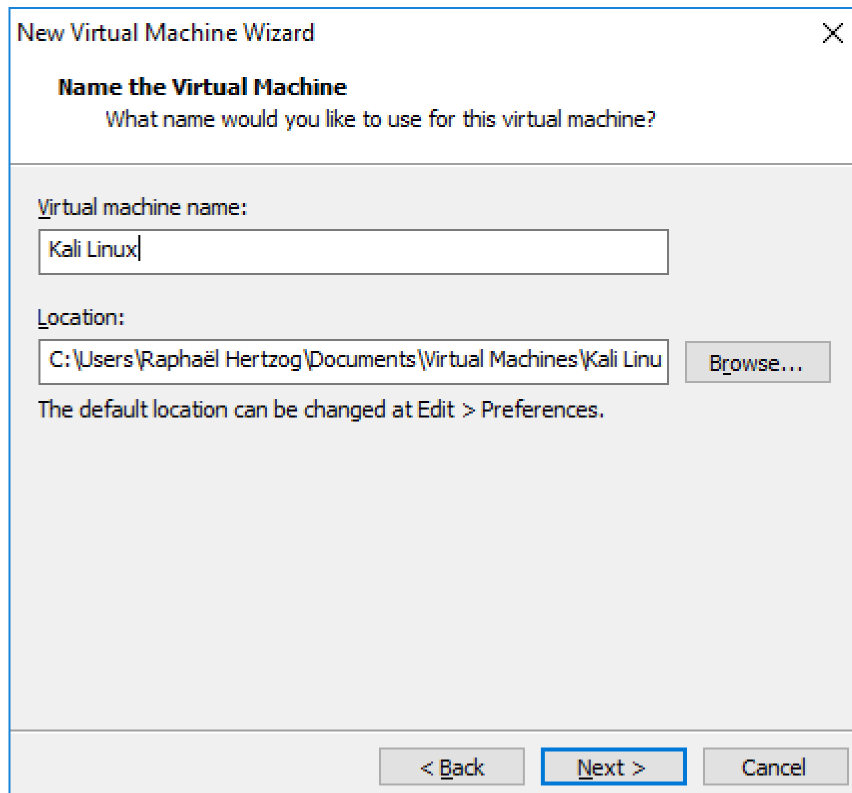
شكل ٢٠.٢ تثبيت نظام التشغيل

يفترض المعالج أنك تريد تثبيت نظام التشغيل على الفور ويطلب منك تحديد صورة ISO التي تحتوي على برنامج التثبيت (الشكل ٢٠.٢، "تثبيت نظام التشغيل"). اختر " Installer disc image file (iso) " وانقر فوق "**Browse**" لتحديد ملف الصورة.



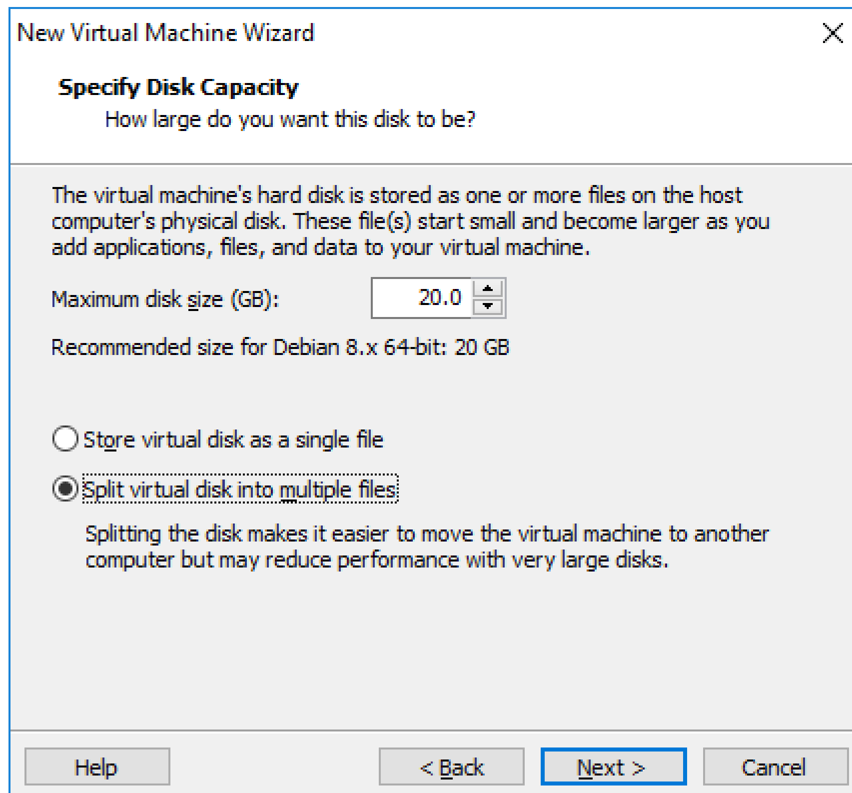
شكل ٢١.٢ اختيار نظام التشغيل

عندما يتعذر اكتشاف نظام التشغيل (OS) من صورة ISO المحددة، يسألك المعالج عن نوع نظام التشغيل الذي تنوي تشغيله. يجب عليك اختيار "Linux" لنظام التشغيل و "Debian 8.x" للإصدار، كما هو مبين في الشكل ٢١.٢، "اختيار نظام التشغيل".



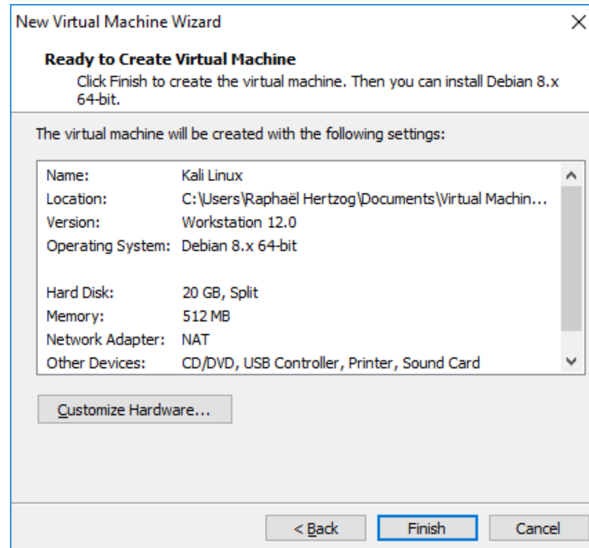
شكل ٢٢.٢ اسم الجهاز الافتراضي

لقد اخترنا Kali Linux كاسم للجهاز الافتراضي الجديد (الشكل ٢٢.٢، "اسم الجهاز الافتراضي"). كما هو الحال مع VirtualBox، لديك أيضًا خيار تخزين ملفات VM في موقع بديل.



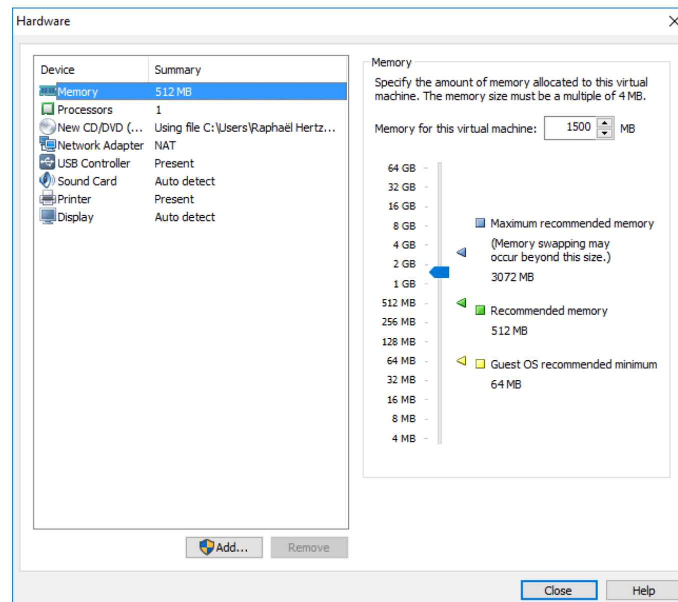
شكل ٢٣.٢ تحديد سعة القرص

عادةً ما يكون حجم القرص الثابت الافتراضي وهو 20 GB (الشكل ٢٣.٢، "تحديد سعة القرص") كافياً ولكن يمكنك ضبطه هنا وفقًا لاحتياجاتك الخاصة. على عكس VirtualBox، والذي يمكنه استخدام ملف واحد بحجم مختلف، فإن VMware لديه القدرة على تخزين محتوى القرص على ملفات متعددة. في كلتا الحالتين، يكون الهدف هو الحفاظ على مساحة قرص نظام التشغيل.



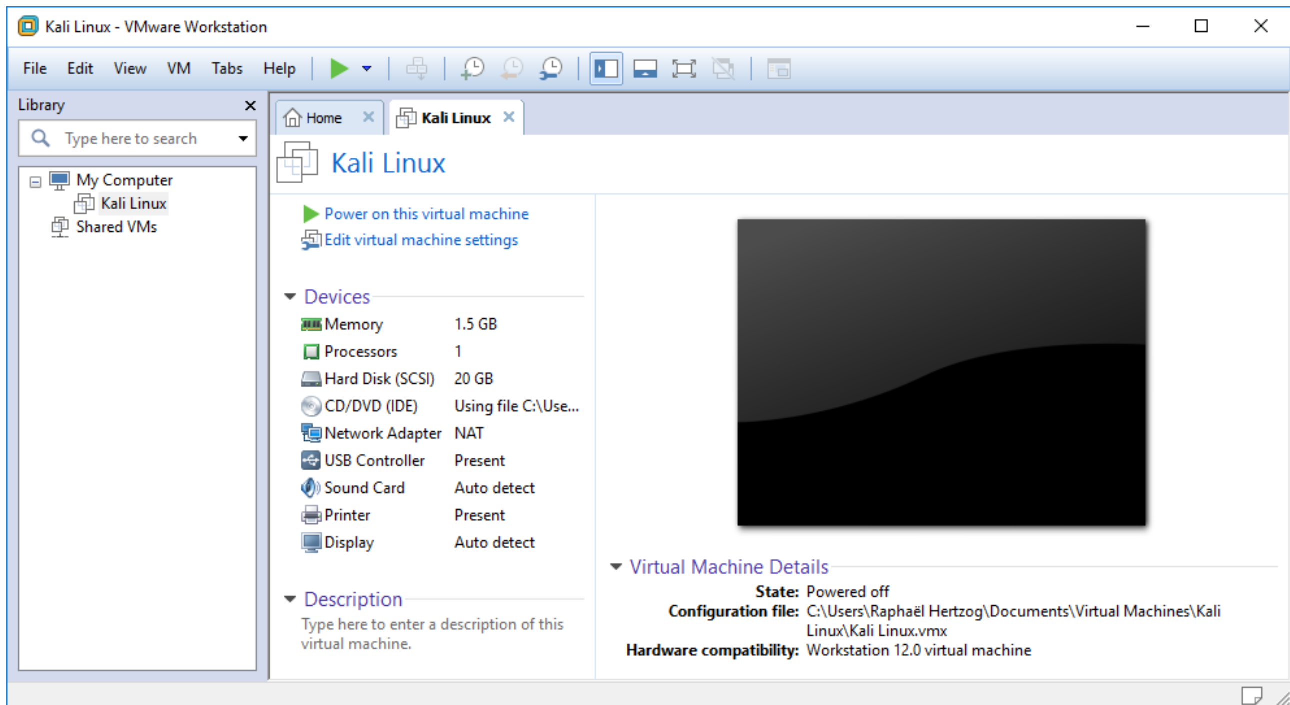
شكل ٢٤.٢ جاهز لإنشاء جهاز افتراضي

تم تكوين VMware Workstation الآن لإنشاء الجهاز الافتراضي الجديد. يعرض ملخصًا للخيارات التي تم إجراؤها حتى تتمكن من التحقق من كل شيء قبل إنشاء الجهاز. ستلاحظ أن المعالج اختار تخصيص MB فقط من ذاكرة الوصول العشوائي للجهاز الافتراضي، وهذا لا يكفي لذلك انقر على ...Customize Hardware (الشكل ٢٤.٢، "جاهز لإنشاء جهاز افتراضي") وقرص إعداد الذاكرة، كما هو مبين في الشكل ٢٥.٢، " نافذة تكوين الهادروير".



شكل ٢٥.٢ نافذة تكوين الهارد وير

بعد نقرة أخيرة على **Finish** (الشكل ٢٤.٢، "جاهز لإنشاء جهاز افتراضي")، تم تكوين الجهاز الافتراضي الآن ويمكن تشغيله بالنقر فوق "Power on this virtual machine" كما هو مبين في الشكل ٢٦.٢، " الجهاز الافتراضي (kali linux) جاهز ".



شكل ٢٦.٢ الجهاز الافتراضي "kali linux" جاهز

٣.٢. الملخص

في هذا الفصل، تعرفنا على مختلف صور Kali Linux ISO وتعلمنا كيفية التحقق منها وتنزيلها، وتعلمنا كيفية إنشاء أقراص USB قابلة للإقلاع من على أنظمة تشغيل مختلفة. ناقشنا أيضًا كيفية تشغيل أقراص USB واستعرضنا كيفية تكوين إعدادات BIOS والإقلاع من وسائط متعددة مختلف، اخترنا وسيط وهو أقراص USB.

نصائح الملخص:

- ❖ www.kali.org هو موقع التنزيل الرسمي الوحيد لـ Kali ISOs. لا تقم بتنزيلها من أي موقع آخر، لأن هذه التنزيلات قد تحتوي على برامج ضارة.
- ❖ تحقق دائمًا من صحة sha256sum للتنزيلات باستخدام الأمر **`sha256sum`** لضمان سلامة تنزيل الصور الخاصة بك. إذا لم يتطابق، فحاول التنزيل مرة أخرى أو استخدم مصدر مختلف.
- ❖ يجب أن تحرق صورة Kali Linux ISO على وسائط قابلة للإقلاع إذا كنت تريد تشغيلها على جهاز حقيقي.
  - ❖ استخدم *Win32 Disk Imager* على Windows.
  - ❖ أو الأداة Disks utility على Linux.
  - ❖ أو الأمر **`dd`** على Mac OS X / macOS.

كن حذرا جدا عند حرق الصورة. قد يؤدي تحديد القرص الخطأ إلى إتلاف البيانات الموجودة على جهازك نهائيًا.

- ❖ قم بتكوين BIOS / UEFI من شاشة الإعدادات وذالك بالضغط على مفتاح Option لنظام OS X / macOS للسماح للجهاز بالاقلاع من محرك USB.

❖ تعد برامج الجهاز الافتراضي مثل *VirhtualBox* و *VMware Workstation Pro* *مفيدة* بشكل خاص إذا كنت ترغب في تجربة Kali Linux ولكنك غير مستعد للالتزام بتثبيته بشكل دائم على جهازك أو إذا كان لديك نظام قوي وتريد تشغيل أنظمة تشغيل متعددة في وقت واحد.

الآن بعد أن تعلمت تثبيت Kali Linux، فقد حان الوقت للتطرق إلى بعض أساسيات Linux المطلوبة لتشغيل Kali الأساسي والمتقدم. إذا كنت من مستخدمي Linux المتوسطين أو المتقدمين، تخطي الفصل التالي.

التمرين الأول للفصل الثاني: إعداد كالي وتنزيله والتحقق منه وحرقه

قم بتثبيت برنامج جهاز إفتراضي (VM)، مثل VMWare Fusion (OSX) أو VirtualBox، أو غيره.

قم بتنزيل إصدار Kali Linux VM (حبذا لو يكون 64 bit).

قم بإقلاع نظام كالي الافتراضي

من هذه النقطة، يجب أن تكون في VM. تسجيل الدخول إلى VM (toor/root) ونزل صورة kali 64-bit من https://www.kali.org/downloads في Kali VM الخاص بك.

قم بتنزيل واستيراد مفاتيح kali العامة.

استخرج بصمات الإصبع (fingerprint) واحصل على SHA256SUMS وملف التوقيع المقترن مع صورة kali.

تحقق من أن المجموع الإختباري لصورة كالي التي قمت بتنزيلها متطابقة تماما مع المجموع الإختباري الموجود في موقع كالي.

أنشئ جهاز USB قابل للإقلاع بالصورة التي عندك.

الإجابات:

يجب ألا تحتاج للمساعدة في تثبيت برنامج VM.

يجب ألا تحتاج للمساعدة في تنزيل نظام كالي، إذا احتجت للمساعدة في هذا، فهذه الدورة ليست لك.

قم باستخراج ملف Kali VM .7z.

نزل صورة نظام كالي، لاحظ أنه خلال هذا التمرين، قد تختلف أرقام نسختك:

```
wget http://cdimage.kali.org/kali-2017.1/kali-linux-2017.1-amd64.iso
```

نزل واستخرج مفاتيح كالي العامة:

```
wget -q -O - https://www.kali.org/archive-key.asc | gpg --import
```

استخرج بصمات الإصبع واحصل على المجموع الإختباري للصورة.

```
gpg --fingerprint 44C6513A8E4FB3D30875F758ED444FF07D8D0BF6
wget http://cdimage.kali.org/kali-2017.1/SHA256SUMS
wget http://cdimage.kali.org/kali-2017.1/SHA256SUMS.gpg
```

الأن، سوف تحقق من التوقيع، لمعرفة ما إذا كان ملف المجموع الإختباري أصلي:

```
gpg --verify SHA256SUMS.gpg SHA256SUMS
```

يجب أن تشاهد تأكيداً: "توقيع جيد"

لكن انتظر، هناك تحذير قبيح يخيفني!

```
gpg: WARNING: This key is not certified with a trusted signature!
```

* ترجمة: هذا المفتاح غير معتمد بتوقيع موثوق به!*

هذا التحذير طبيعي. يمكنك تجنب ذلك باستخدام خيار "الثقة دائمًا".

-trust-model always

يقول التحذير فقط أنه لا يوجد طريق بين مجموعة المفاتيح الموثوقة ومفتاح Kali في شبكة الثقة. إذا لم يكن لديك أي مفتاح و/أو إذا لم توقع أبدًا على أي شخص آخر، فلن تتمكن أبدًا من الحصول على مسار ثقة لأي مفتاح آخر.

الآن بعد أن تعرف أن ملف SHA256SUMS أصلي، يمكنك الوثوق بالتجزئة الموجودة في هذا الملف. الآن، احصل على مجموع SHA من ISO الذي قمت بتنزيله:

```
root@kali:~# shasum -a 256 ./kali-linux-2017.1-amd64.iso
49b1c5769b909220060dc4c0e11ae09d97a270a80d259e05773101df62e11e9d  ./kali-linux-2017.1-amd64.iso
```

قارن الهاش الخاصة بك مع الهاش المدرج في ملف المجموع الاختباري (موثوق به الان):

```
root@kali:~# grep kali-linux-2017.1-amd SHA256SUMS
49b1c5769b909220060dc4c0e11ae09d97a270a80d259e05773101df62e11e9d  kali-linux-2017.1-amd64.iso
```

إذا لم يتطابق الهاشان، فقد ارتكبت خطأً (أو حدث لك شيء خاطئ!).

ضع محرك USB الخاص بك، وقم بوصله في VM، وابحث عنه باستخدام **dmesg**، واحرق الصورة القابلة للإقلاع باستخدام شيء مثل هذا. توخ الحذر! هذا مدمر! استخدم مسار القرص الصحيح (/dev/sdb في حالتنا)!

```
root@kali:~# dmesg
[٤١١٧,١٣٢٨١١ ]usb 1-1: new high-speed USB device number 2 using ehci-pci
[٤١١٧,٢٨٧٣١٩ ]usb 1-1: New USB device found, idVendor=0781, idProduct=5583
[٤١١٧,٢٨٧٣٢١ ]usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[٤١١٧,٢٨٧٣٢٢ ]usb 1-1: Product: Ultra Fit
[٤١١٧,٢٨٧٣٢٢ ]usb 1-1: Manufacturer: SanDisk
[٤١١٧,٢٨٧٣٢٣ ]usb 1-1: SerialNumber: 4C530001231103111240
[٤١١٧,٤٠٧٩٠٢ ]usb-storage 1-1:1.0: USB Mass Storage device detected
[٤١١٧,٤٠٨٨٥٥ ]scsi host3: usb-storage 1-1:1.0
[٤١١٧,٤١٠٣٧٠ ]usbcore: registered new interface driver usb-storage
[٤١١٧,٤٦٥٣٨٦ ]usbcore: registered new interface driver uas
[٤١١٨,٤٢١٣٠٨ ]scsi 3:0:0:0: Direct-Access    SanDisk  Ultra Fit       1.00 PQ: 0 ANSI: 6
[٤١١٨,٤٢٩١٠٧ ]sd 3:0:0:0: Attached scsi generic sg2 type 0
[٤١١٨,٤٣٢١٥١ ]sd 3:0:0:0: [sdb] 242614272 512-byte logical blocks: (124 GB/116 GiB(
[٤١١٨,٤٣٨٧٠٩ ]sd 3:0:0:0: [sdb] Write Protect is off
[٤١١٨,٤٣٨٧١٣ ]sd 3:0:0:0: [sdb] Mode Sense: 43 00 00 00
[٤١١٨,٤٤١٩٦٩ ]sd 3:0:0:0: [sdb] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA
[٤١١٨,٤٦٨٩٠٣ ]sdb: sdb1
[ 4118.492354] sd 3:0:0:0: [sdb] Attached SCSI removable disk
root@kali:~# dd if=kali-linux-2017.1-amd64.iso of=/dev/sdb bs=1M
```

2664+1 records in

2664+1 records out

2794307584 bytes (2.8 GB, 2.6 GiB) copied, 93.8987 s, 29.8 MB/s

غذاء الفكر:

ما هي فوائد الإقلاع المباشرة التي يمكنك التفكير بها؟ وما هي الفوائد السيئة؟

سؤال زن لهذا اليوم:

هل يصيبك غرابة أنه يمكنك ببساطة إدخال ISO إلى مفتاح USB والإقلاع منه؟

الإجابة:

يعد Kaliبالإقلاع المباشر رائعًا عندما تريد:

- ❖ الاحتفاظ بنسخة محمولة من Kali في جيبك.
- ❖ اختبار Kali Linux دون إجراء أي تغييرات على جهاز الحاسوب الخاص بك.
- ❖ بحاجة إلى وضع التحقيق الجنائي.

إجابة سؤال زن: كالي (ودبيان) ISO هي صورة هجينة "**isohybrid**". عندما يتم بناء ISO، تقوم الأداة المساعدة syslinux بتشغيل الأمر ***isohybrid*** على ISO، الذي يضيف جزء مجدول إلى ISO، بينما لا يزال يحتفظ به ملف ISO صالح.

التمرين الثاني للفصل الثاني: إقلاع Kali

١. قم بتشغيل محرك Kali USB الذي قمت بإنشائه في التمرين السابق، واختر الوضع المباشر.

٢. إنشاء ملف 6GB في root/.

٣. ماذا حدث ولماذا؟

٤. تحقق من أن التغييرات لا تستمر في الوضع المباشر عن طريق إعادة التشغيل.

الإجابة:

١. هناك عدة طرق للقيام بهذا. يمكنك إعادة تشغيل الجهاز المضيف الخاص بك، والإقلاع من USB. يمكنك أيضًا الإقلاع من VirtualBox باستخدام USB (ابحث في قوقل عن "boot usb virtualbox ") أو يمكنك تشغيل USB من برنامج VMWare. راجع مقالة kali.org لمزيد من المعلومات حول إقلاع USB من برنامج VMWare.

٢. لإنشاء ملف بحجم 6 GB:

```
dd if=/dev/zero of=test.img bs=1M count=6144
```

٣. في النهاية، ستتلقى رسالة تفيد بأنه "لا توجد مساحة على الجهاز"، على الرغم من أنك قمت بتكوين محرك أقراص ثابت سعة 20 GB ... ماذا حدث؟ حسنًا، نظرًا لأنك في الوضع المباشر، فأنت تعمل في ذاكرة الوصول العشوائي. لذلك كل ما تفعله في "نظام الملفات" يكتب في نهاية المطاف في ذاكرة عشوائية. بمجرد نفاد ذاكرة الوصول العشوائي (RAM) ... تنفد مساحة القرص.



٤. أعد التشغيل، وتحقق من التغيرات التي أجريتها.

التمرين الثالث للفصل الثاني: تعديل مدخلات الإقلاع

١. لقد قمنا بالإقلاع من Kali VM أنشأناه مسبقا ومحرك Kali USB. الآن، سنقوم بتشغيله بطريقة أخرى. إقلاع VM من ISO kali. تأكد من أن الشبكة في وضع NAT.
٢. قم بتحرير خيار الإقلاع المباشر وأضف الخيار "الصامت (quiet)" على سطر النواة للحصول على إقلاع أقل مطوّل لأعلى.
٣. تأكد من أن هذا يحدث فرقًا في لفظ إقلاع.
٤. تحقق من معلمات الإقلاع في الوضع المباشر والتحقيق الجنائي. ما هي الاختلافات؟

الإجابات:

للإقلاع من ISO، قم بتوصيل Kali ISO بمحرك الأقراص المضغوطة الافتراضي قبل التشغيل.

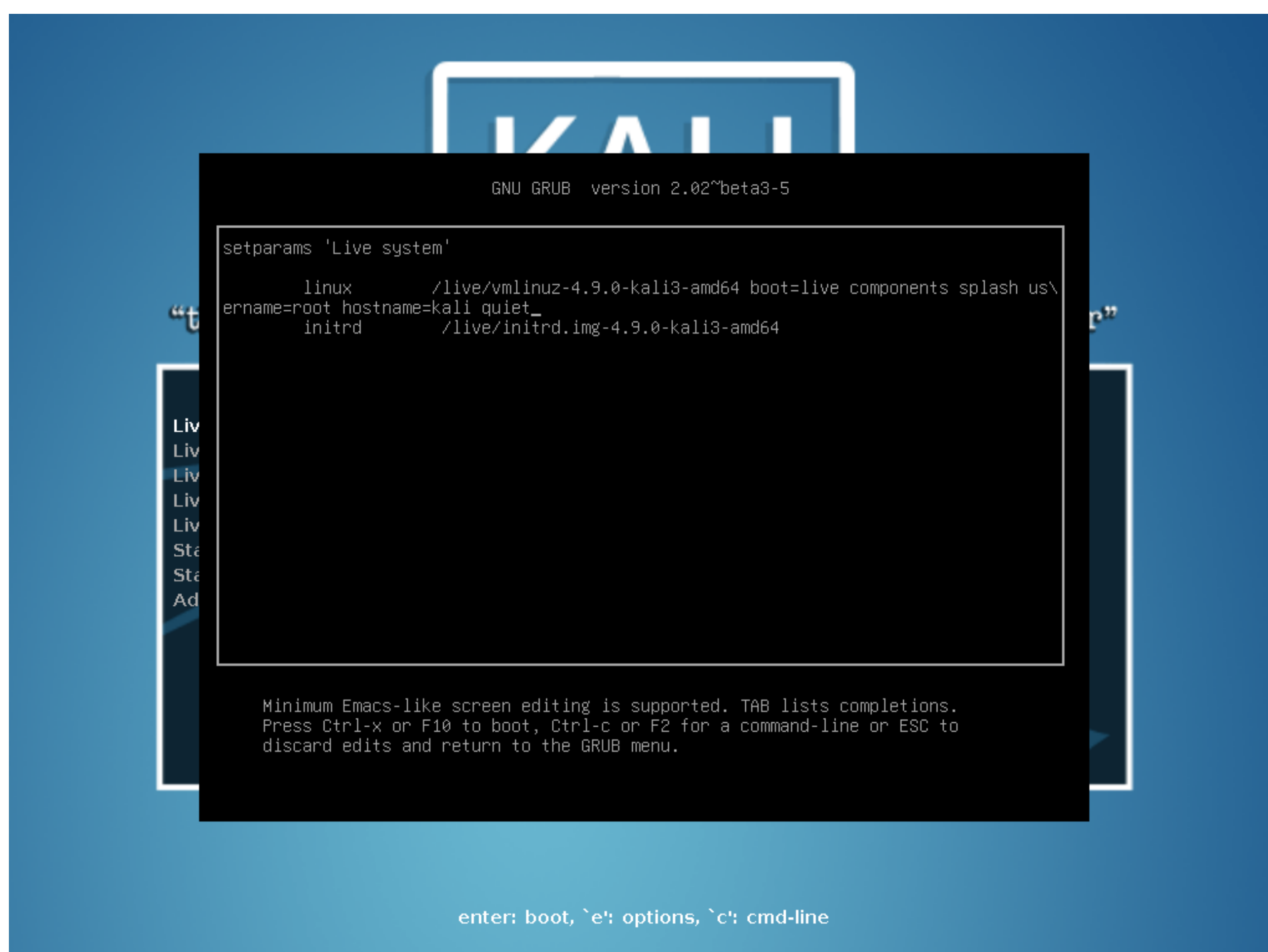
في VMWare، يوجد هذا في:

Virtual Machine > Settings > CD/DVD (IDE)

حدد المربع لتمكين القرص المضغوط، وحدد صورة القرص. لتمكين وضع NAT: في

VMWare> Virtual Machine> Network Adapter

في قائمة الإقلاع، اختر الإقلاع المباشر، واضغط على e وأضف "quiet" إلى سطر linux:



الإقلاع بـ ctrl-x أو f10.

فعلتها؟

الاختلافات في noswap **ومعلمات الإقلاع** noautomount **والتي توجد في خيار وضع التحقيق الجنائي.**

في حين أن noswap هي معلمة إقلاع ديبيان قياسية، فإن noautomaount هي ميزة محددة من Kali، يتم تنفيذها بواسطة ملف /etc/X11/Xsession.d/52kali_noautomount/، والتي يتم شحنها في حزمة kali-defaults.

اختبار الشهادة للفصل الثاني

السؤال الأول:

إذا كان لديك سطح مكتب Intel 64-bit، فما صورة كالي التي ستقوم بتشغيلها على جهازك؟ اختر كل ما ينطبق.

- ☐ Kali 32-bit
- ☐ Kali armhf
- ☐ Kali 64-bit
- ☐ Kali armel

السؤال الثاني:

ما الملف الافتراضي الذي يمكنك التحقق منه لتحديد ما إذا كانت وحدة المعالجة المركزية في جهاز Kali Linux الخاص بك هي 32 أو 64 bit؟

- ☐ /proc/cpuflags
- ☐ /proc/cpu
- ☐ /proc/system
- ☐ /proc/cpuinfo

السؤال الثالث:

ما الأمر الذي سيقوم بتنزيل واستيراد مفتاح كالي العام عبر https؟

- ☐ **gpg_import** https://www.kali.org/archive-key.asc
- ☐ **echo** archive-key.asc **| gpg -import**
- ☐ **wget -q -O** - https://www.kali.org/archive-key.asc **| gpg -import**
- ☐ **lynx** http://www.kail.org/archive-key.asc **| gpg_import**

السؤال الرابع:

عند تثبيت Kali Linux على جهاز افتراضي، ما هي طريقة التثبيت التي من المحتمل أن تنتج تثبيتًا نظيفًا؟

- ☐ تنزيله من الموقع الرسمي، التحقق من صورة Kali 32-bit وحرقه على USB.
- ☐ تنزيله من الموقع الرسمي، التحقق من صورة Kali 32-bit ISO وحرقه على USB باستخدام ملف preeseed.cfg الرسمي.
- ☐ تنزيله من الموقع الرسمي، والتحقق من صورة Kali VM.
- ☐ استيراد المثبتة مسبقا، التحقق من صحة واختبار جهاز Kali 32-bit.

الإجابات:

إجابة السؤال الأول:

Kali 32-bit and Kali 64-bit

إجابة السؤال الثاني:

/proc/cpuinfo

إجابة السؤال الثالث:

```
wget -q -O - https://www.kali.org/archive-key.asc
| gpg -import
```

إجابة السؤال الرابع:

تنزيله من الموقع الرسمي، والتحقق من صورة Kali VM.

---((الفصل الثالث))---

٣. أساسيات لِينِكس

قبل أن تتمكن من إتقان Kali Linux، يجب أن تكون مرتاحًا باستخدام نظام Linux. سوف تفيدك الخبرة في نظام Linux، لأنه يمثل نسبة كبيرة من الويب والبريد الإلكتروني وخدمات الإنترنت الأخرى التي تعمل بخوادم Linux.

في هذا الفصل، نسعى جاهدين لتغطية أساسيات Linux، لكننا نفترض أنك تعرف بالفعل أنظمة الحاسوب بشكل عام، بما في ذلك المكونات مثل وحدة المعالجة المركزية (CPU) وذاكرة الوصول العشوائي (RAM) واللوحة الأم والقرص الصلب، بالإضافة إلى وحدات التحكم بالأجهزة والموصلات المرتبطة بها.

١.٣. ما هو لينكس وماذا يفعل؟

غالبًا ما يستخدم مصطلح "Linux" للإشارة إلى نظام التشغيل بالكامل، ولكن في الواقع، Linux هو نواة نظام تشغيل فقط، والذي يتم تشغيله بواسطة أداة محمل الإقلاع، والتي يتم تشغيلها هي نفسها بواسطة BIOS/UEFI. تمثل النواة دورًا مشابهًا لدور موصل في الأوركسترا — فهي تضمن التنسيق بين العتاد والبرامج. يتضمن هذا الدور إدارة الأجهزة والعمليات والمستخدمين والأذونات ونظام الملفات. توفر النواة (kernel) قاعدة مشتركة لجميع البرامج الأخرى الموجودة على النظام وعادةً ما يتم تشغيله في *حلقة الصفر* (*Ring Zero*)، والمعروفة أيضًا باسم مساحة النواة.

مساحة المستخدم

نحن نستخدم مصطلح مساحة المستخدم لجمع كل ما يحدث خارج النواة معًا.

من بين البرامج التي يتم تشغيلها في مساحة المستخدم العديد من الأدوات الأساسية من مشروع GNU، ومعظمها يهدف إلى تشغيلها من سطر الأوامر. يمكنك استخدامها في البرامج النصية لأتمتة العديد من المهام.

لنراجع سريعا المهام المختلفة التي تعالجها نواة لينكس:

١.١.٣. التحكم في العتاد

النواة مكلفة (تعطي الأوامر)، أولاً وقبل كل شيء، بالتحكم في مكونات أجهزة الحاسوب. تكتشفها وتقوم بتكوينها عند تشغيل الحاسوب، أو عند إدخال جهاز أو إزالته (على سبيل المثال، جهاز USB). كما أنها تتيحها للبرامج عالية المستوى، من خلال واجهة برمجة مبسطة، بحيث يمكن للتطبيقات الاستفادة من الأجهزة دون الحاجة إلى معالجة تفاصيل مثل فتحة التمديد التي يتم توصيل لوحة الخيارات بها. توفر واجهة البرمجة أيضًا طبقة تجريدية. يتيح ذلك لبرنامج محادثات الفيديو، على سبيل المثال، استخدام كاميرا ويب بغض النظر عن مصنعها وطرازها. يمكن للبرنامج استخدام واجهة (Video for Linux (V4L وستقوم النواة بترجمة المكالمات الوظيفية للواجهة إلى أوامر العتاد التي تحتاجها كاميرا الويب المحددة المستخدمة.

تقوم النواة بتصدير بيانات حول الأجهزة المكتشفة من خلال أنظمة الملفات الإفتراضية **/proc/** و **/sys/**. غالبًا ما تصل التطبيقات إلى الهاردوير عن طريق الملفات التي يتم إنشاؤها داخل **/dev/**. تمثل ملفات معينة محركات الأقراص (على سبيل المثال، **dev/sda/**)، والأجزاء (**dev/sda1/**)، والفأرة (**dev/input/mouse0/**)، ولوحات المفاتيح (**dev/input/event0/**)، وكرت الصوت (**/*dev/snd/**)، المنافذ التسلسلية (**dev/ttyS*/**)، والمكونات الأخرى.

هناك نوعان من ملفات الإجهزة: *الكتلة والحرف* (*block* and *character*).

خصائص الكتلة: لديها حجم محدود، ويمكنك الوصول للبايتات في أي موضع في الكتلة.

خصائص الحرف: يمكنك قراءة الأحرف وكتابتها، لكن لا يمكنك البحث عن وظيفة معينة وتغيير وحدات البايت التعسفية.

لمعرفة نوع ملف جهاز معين، انظر للحرف الأول من إخراج أمر:

```
ls -l
```

b: لأجهزة الكتلة، و **c**: لأجهزة الأحرف:

```
$ ls -l /dev/sda /dev/ttyS0
brw-rw---- 1 root disk    8,  0 Mar 21 08:44 /dev/sda
crw-rw---- 1 root dialout 4, 64 Mar 30 08:59 /dev/ttyS0
```

كما ترى، تستخدم محركات الأقراص والأجزاء أجهزة الكتلة، بينما تستخدم الفأرة ولوحة المفاتيح والمنافذ التسلسلية أجهزة الأحرف. في كلتا الحالتين، تتضمن واجهة البرمجة أوامر خاصة بالجهاز والتي يمكن استدعاءها من خلال نظام يسمى *ioctl*.

٢.١.٣ توحيد أنظمة الملفات

أنظمة الملفات هي جانب بارز في النواة. تقوم الأنظمة المشابهة لـ Unix بدمج جميع مخازن الملفات في تسلسل هرمي واحد، مما يتيح للمستخدمين والتطبيقات الوصول إلى البيانات من خلال معرفة موقعها داخل هذا التسلسل الهرمي.

تسمى نقطة الانطلاق لهذه الشجرة الهرمية الجذر(root)، ويمثلها الحرف "/". يمكن أن يحتوي هذا المجلد على مجلدات فرعية. على سبيل المثال، يسمى المجلد الفرعي **الرئيسي** بـ **/home/**. يمكن لهذا المجلد الفرعي أن يحتوي على مجلدات فرعية أخرى، وما إلى ذلك. يمكن أن يحتوي كل مجلد أيضًا على ملفات، حيث سيتم تخزين البيانات. وبالتالي، يشير **/home/buxy/Desktop/hello.txt** إلى ملف يسمى **hello.txt** المخزّن في المجلد الفرعي Desktop والذي هو داخل المجلد الفرعي buxy للمجلد الرئيسي، الموجود في الجذر. تترجم النواة بين نظام التسمية هذا وموقع التخزين على القرص.

بخلاف الأنظمة الأخرى، يمتلك Linux تسلسل هرمي واحد فقط، ويمكنه دمج البيانات من عدة أقراص. يصبح أحد هذه الأقراص هو الجذر، ويتم *وصل* الأقراص الأخرى بالمجلدات في التسلسل الهرمي. (يُطلق على هذا الأمر في Linux **`mount`**) هذه الأقراص الأخرى متوفرة بعد ذلك ضمن نقاط الوصل (mount point). يتيح ذلك تخزين المجلدات الرئيسية للمستخدمين (يتم تخزينها تقليديًا داخل /home/) على قرص ثابت مجزء، والذي سيحتوي على مجلد **buxy** (إلى جانب المجلدات الرئيسية للمستخدمين الآخرين). بمجرد وصل القرص على **/home/**، تصبح هذه المجلدات قابلة للوصول في مواقعها المعتادة، وتستمر المسارات مثل **/home/buxy/Desktop/hello.txt** في العمل.

هناك العديد من تنسيقات نظام الملفات، والتي تقابل العديد من الطرق لتخزين البيانات فعلياً على الأقراص. الأكثر شهرة على نطاق واسع هي *ext2* و *ext3* و *ext4*، ولكن يوجد غيرها. على سبيل المثال، *VFAT* هو نظام الملفات الذي تم استخدامه تاريخيا من قبل أنظمة التشغيل DOS وWindows. يتيح دعم Linux لنظام VFAT إمكانية الوصول إلى الأقراص الصلبة تحت Kali وكذلك في Windows. على أي حال، يجب عليك إعداد نظام ملفات على القرص قبل أن تتمكن من وصله وتُعرف هذه العملية باسم التنسيق (*formatting*). باستخدام أوامر مثل **mkfs.ext3** (حيث **mkfs** اختصار لـ **M**a**K**e **F**ile**S**ystem) تتعامل مع التنسيق. تتطلب هذه الأوامر، كمعلمة، ملف جهاز يمثل الجزء المراد تنسيقه (على سبيل المثال، **/dev/sda1**، الجزء الأول على محرك الأقراص الأول). هذه العملية مدمرة ويجب تشغيلها مرة واحدة فقط، إلا إذا كنت تريد مسح نظام الملفات والبدء من جديد.

هناك أيضًا أنظمة ملفات الشبكة مثل (network filesystems) NFS، التي لا تخزن البيانات على قرص محلي. ولكن بدلا من ذلك، تنقل البيانات عبر الشبكة إلى خادم يقوم بتخزينها واستردادها عند الطلب. بفضل تجريد نظام الملفات، لا داعي للقلق بشأن كيفية الوصول لهذا القرص، حيث تظل الملفات قابلة للوصول بطريقتها الهرمية المعتادة.

٣.١.٣. إدارة العمليات

العملية عبارة عن مثيل قيد التشغيل لبرنامج، والذي يتطلب ذاكرة لتخزين كل من البرنامج نفسه وبيانات التشغيل الخاصة به. النواة هي المسؤولة عن إنشاء وتتبع العمليات. عند تشغيل البرنامج، تقوم النواة أولاً بتخصيص بعض الذاكرة جانبًا، وتقوم بتحميل الكود القابل للتنفيذ من نظام الملفات فيه، ثم يبدأ تشغيل التعليمات البرمجية. يحتفظ بمعلومات حول هذه العملية، وأبرزها هو رقم التعريف المعروف باسم معرف العملية (*process identifier*) (PID).

مثل معظم أنظمة التشغيل الحديثة، فإن تلك التي لها نواة تشبه يونكس، بما في ذلك لينكس، قادرة على تعدد المهام. بمعنى آخر، فهي تسمح للنظام بتشغيل العديد من العمليات في نفس الوقت. هناك بالفعل عملية واحدة قيد التشغيل في أي وقت واحد، لكن النواة تقسم وقت وحدة المعالجة المركزية إلى شرائح صغيرة وتقوم بتشغيل كل عملية بدورها. نظرًا لأن هذه الشرائح الزمنية قصيرة جدًا (في نطاق المللي ثانية)، فإنها تخلق مظهر العمليات التي تعمل بشكل متوازٍ، على الرغم من أنها نشطة فقط خلال الفاصل الزمني الخاص بها وتتوقف عن العمل بقية الوقت. تتمثل مهمة النواة في ضبط آليات الجدولة للحفاظ على هذا المظهر، مع زيادة أداء النظام إلى أقصى حد. إذا كانت شرائح الوقت أطول من اللازم، فقد لا يظهر التطبيق سريع الاستجابة حسب الرغبة. قصير جدًا، ويفقد النظام الوقت عن طريق تبديل المهام كثيرًا جدًا. يمكن تحسين هذه القرارات بأولويات العملية، حيث سيتم تشغيل العمليات ذات الأولوية العليا لفترات أطول وبشرائح زمنية أكثر تكرارًا من العمليات ذات الأولوية المنخفضة.

المعالجات المتعددة (والمتغيرات)

لا يتم تطبيق القيد الموضح أعلاه، وهو عملية واحدة فقط يتم تشغيلها في كل مرة، دائمًا: القيد الفعلي هو أنه لا يمكن أن يكون هناك سوى عملية واحدة قيد التشغيل لكل نواة معالج. تسمح الأنظمة متعددة المعالجات، أو متعددة النواة، أو ذات العمليات المتعددة، بتشغيل عدة عمليات بشكل متوازٍ. ومع ذلك، يتم استخدام نظام تقطيع الوقت نفسه لمعالجة الحالات التي توجد فيها عمليات أكثر نشاطًا من مراكز المعالج المتوفرة. هذا ليس بالأمر غير المعتاد: النظام الأساسي، حتى لو كان خاملاً في الغالب، يحتوي دائمًا على عشرات العمليات الجارية.

تسمح النواة بتشغيل عدة مثيلات مستقلة لنفس البرنامج، لكن يُسمح لكل منها بالوصول فقط إلى شرائح الوقت والذاكرة الخاصة به. وبالتالي تبقى بياناتهم مستقلة.

٤.١.٣. إدارة الحقوق

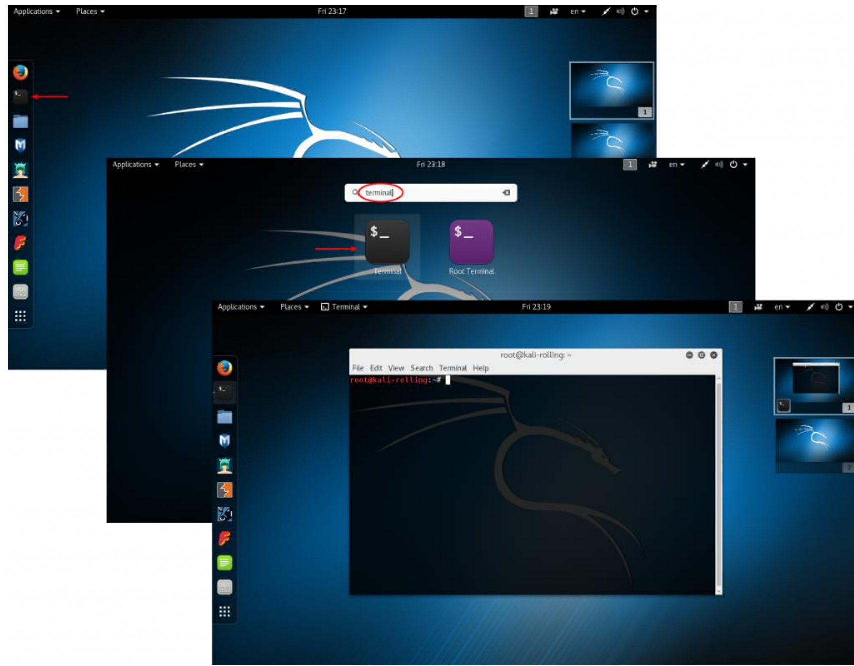
تدعم الأنظمة الشبيهة بيونكس العديد من المستخدمين والمجموعات وتسمح بالتحكم في الأذونات. في معظم الأحيان، يتم تحديد عملية من قبل المستخدم الذي بدأها. لا يُسمح بهذه العملية إلا باتخاذ الإجراءات المسموح بها لمالكها. على سبيل المثال، يتطلب فتح ملف من النواة التحقق من هوية العملية مقابل أذونات الوصول (لمزيد من التفاصيل حول هذا المثال بالذات، انظر باب ٤.٤.٣، "إدارة الحقوق").

٢.٣. سطر الأوامر

نعني بكلمة سطر الأوامر واجهة تعتمد على النصوص، تتيح لك إدخال الأوامر وتنفيدها وعرض النتائج. يمكنك تشغيل الـ(terminal) (شاشة نصية داخل سطح المكتب الرسومي، أو وحدة التحكم في النص نفسها خارج أي واجهة رسومية) الذي يحتوي على مترجم أوامر (shell).

١.٢.٣. كيفية الوصول لسطر الأوامر

عندما يعمل النظام بشكل صحيح، فإن أسهل طريقة للوصول لسطر الأوامر هي تشغيل الـ (terminal) في سطح المكتب.



شكل ١.٣ "بدء تشغيل Gnome terminal"

على سبيل المثال، على نظام kali linux الافتراضي، يمكن تشغيل Gnome Terminal من قائمة التطبيقات المفضلة، يمكنك أيضا كتابة كلمة "**terminal**" أثناء وجودك في شاشة الأنشطة (تلك التي يتم تنشيطها عند تحريك الماوس إلى الزاوية العلوية اليسرى) والنقر على أيقونة التطبيق الصحيح التي تظهر (الشكل ١.٣ "بدء تشغيل Gnome terminal").

في حالة تعطل الواجهة الرسومية الخاصة بك، لا يزال بإمكانك الحصول على واجهة سطر الأوامر بواسطة وحدات التحكم الافتراضية (يمكن الوصول إلى ستة منها من خلال مجموعات المفاتيح الستة CTRL + ALT + F1 إلى - CTRL + ALT + F6 مفتاح CTRL يمكن حذفه إذا كنت بالفعل في شاشة سطر الأوامر، خارج واجهة Xorg أو Wayland الرسومية). يمكنك الحصول على شاشة تسجيل دخول أساسية حيث تدخل معلومات تسجيل الدخول وكلمة المرور الخاصة بك قبل منحك حق الوصول لسطر الأوامر باستخدام الصدفة (shell):

```
Kali GNU/Linux Rolling kali-rolling tty3
kali-rolling login: root
Password:
Last login: Fir Mar 25 12:30:05 EDT 2016 from 192.168.122.1 on pts/2
Linux kali-rolling 4.4.0-kali1-amd4 #1 SMP Debian 4.4.6-1kali1
(2016-03-18) x86_64
The programs included with the Kali GNU/Linux system are free
software؛
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali-rolling#~:
```

يُطلق على البرنامج الذي يتعامل مع المدخلات وتنفيذ الأوامر الخاصة بك اسم shell (أو مترجم سطر أوامر).

shell الافتراضي لـ Kali Linux هو Bash (وهو اختصار لـ *Bourne Again Shell*). تشير الـ "**$**" أو "**#**" إلى أن الصدفة تنتظر المدخلات الخاصة بك. يشير أيضًا إلى ما إذا كان Bash يتعرف عليك كمستخدم عادي (**$**) أو كمستخدم فائق (**#**).

٢.٢.٣. أساسيات سطر الأوامر: تصفح شجرة المجلدات وإدارة الملفات

هذا الفصل يعطي فقط نظرة عامة مختصرة على بعض الأوامر، والتي تحتوي جميعها على العديد من الخيارات غير مذكورة هنا، لذا يرجى الرجوع إلى الوثائق الوفيرة المتوفرة في صفحاتها اليدوية. في اختبارات الاختراق، ستحصل غالبًا على وصول shell إلى نظام بعد استغلال ناجح، بدلاً من واجهة مستخدم رسومية. الكفاءة في سطر الأوامر أمر ضروري لنجاحك كمحترف أمني.

|| أقترح عليك قراءة الكتاب المترجم "سطر أوامر لينكس" ||

بمجرد فتح الجلسة:

يعرض الأمر **pwd** (الذي هو اختصار لـ print working directory) موقعك الحالي في نظام الملفات.

يتم تغيير المجلد الحالي باستخدام الأمر:

cd *(اسم أو مسار المجلد)*

cd اختصار لـ(*Change Directory*) عندما لا تحدد المجلد الهدف، يتم نقلك إلى المجلد الرئيسي. عند كتابة أمر **- cd**، ستعود إلى مجلد العمل السابق (المجلد المستخدم قبل اجراء أمر **cd**). يعرف المجلد الأب دائما بـ **..** (نقطتان)، في حين يُعرف المجلد الحالي أيضًا باسم **.** (نقطة واحدة). يسمح الأمر **ls** بسرد محتويات المجلد. إذا لم تكتب معلمات، فسوف تعمل على المجلد الحالي.

```
$pwd
    /home/buxy
$cd Desktop
$pwd
    /home/buxy/Desktop
$cd .
$pwd
    /home/buxy/Desktop
$cd ..
$pwd
/home/buxy
$ls
Desktop     Downloads  Pictures  Templates
Documents   Music      Public    Videos
```

يمكنك إنشاء مجلد جديد باستخدام أمر:

mkdir *(اسم المجلد)*

وإزالة مجلد موجود (فارغ) باستخدام أمر:

rmdir *(اسم المجلد)*

يتيح الأمر **mv** نقل وإعادة تسمية الملفات والمجلدات.

يتم إزالة ملف باستخدام الأمر:

rm *(اسم الملف)*

ويتم نسخ ملف باستخدام الأمر:

cp *(اسم الملف الأصل)* *(اسم الملف الهدف)*

```
$mkdir test
$ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    test
$mv test new
$ls
Desktop    Downloads  new       Public     Videos
Documents  Music      Pictures  Templates
$rmdir new
$ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public
```

تنفّذ الصدفة كل أمر عن طريق تشغيل البرنامج الأول بالاسم المحدد الذي يعثر عليه في المجلد المدرج في بيئة المسار المتغير **PATH**. في معظم الأحيان، تكون هذه البرامج في **bin/** أو **sbin/** أو **usr/bin/** أو **usr/sbin/**. على سبيل المثال، يوجد الأمر **ls** في **bin/ls/**؛ الأمر **which** يبين موقع الملف القابل للتنفيذ. في بعض الأحيان، يتم التعامل مع الأمر مباشرةً بواسطة الصدفة، في هذه الحالة، يطلق عليه أوامر الصدفة (**cd** و **pwd** من بينهن أيضا)؛ يتيح لك الأمر **type** الاستعلام عن نوع كل أمر.

```
$echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/sbin:/bin
$which ls
/bin/ls
$type rm
rm is /bin/rm
$type cd
cd is a shell builtin
```

لاحظ استخدام الأمر **echo**، والذي يعرض ببساطة النصوص على الـ(terminal). في هذه الحالة، يتم استخدامه لطباعة محتويات متغير بيئة، لأن shell يستبدل المتغيرات تلقائيًا بقيمها قبل تنفيذ سطر الأوامر.

متغيرات البيئة

تسمح متغيرات البيئة بتخزين الإعدادات العامة للصدفة أو البرامج الأخرى المختلفة. فهي سياقية ولكن قابلة للتوريث. على سبيل المثال، تحتوي كل عملية على مجموعة متغيرات البيئة الخاصة بها (فهي سياقية). يمكن أن تقوم الصدفات، مثل صدفة تسجيل الدخول، بإعلان المتغيرات، والتي سيتم نقلها إلى البرامج الأخرى التي تنفذها (وهي قابلة للتوريث).

يمكن تعريف هذه المتغيرات على مستوى النظام في etc/profile/ أو لكل مستخدم في ملف التعريف profile/ ~ ولكن يتم وضع المتغيرات غير الخاصة بمترجمي سطر الأوامر بشكل أفضل في etc/environment/، حيث سيتم حقن هذه المتغيرات في جميع المستخدمين جلسات العمل بفضل وحدة المصادقة القابلة للتوصيل (PAM) - حتى في حالة عدم تنفيذ برنامج shell.

٣.٣. نظام الملفات

١.٣.٣. نظام التسلسل الهرمي القياسي

كما هو الحال في توزيعات linux الأخرى، تم تنظيم kali linux بحيث يتوافق مع معيار *نظام الملفات الهرمي* (FHS)، مما يسمح لمستخدمي توزيعات linux الأخرى بالعثور على مساراتهم بسهولة في kali. يحدد FHS الغرض من كل مجلد، يتم وصف المجلدات كما يلي:

البرامج الأساسية binary	**/bin/**
نواة Kali Linux وملفات أخرى مطلوبة لعملية الإقلاع	**/boot/**
ملفات الجهاز device	**/dev/**
ملفات التكوين et cetera (بمعنى إلخ)	**/etc/**
ملفات المستخدم الشخصية	**/home/**
المكتبات الأساسية library	**/lib/**
نقاط وصل للأجهزة القابلة للإزالة، مثل: (USB, CD-Rom) وغيرها ...	**/media/***
نقاط الوصل المؤقتة mount	**/mnt/**
تطبيقات إضافية optional	**/opt/**
الملفات الشخصية للمسؤول (الجذر)	**/root/**
بيانات وقت التشغيل المتغيرة التي لا تبقى خلال عمليات إعادة التشغيل	**/run/**
برامج النظام system binary	**/sbin/**
البيانات المستخدمة من قبل الخوادم المستضافة على هذا النظام service	**/srv/**
ملفات مؤقتة (غالبا ما يتم إفراغ هذا المجلد عند الإقلاع) temporary	**/tmp/**

/usr/	التطبيقات (هذا المجلد ينقسم إلى **bin**، **sbin**، **lib** وفقًا لنفس المنطق كما في مجلد الجذر) علاوة على ذلك، **/usr/share/** يحتوي على بيانات مستقلة عن الهندسة المعمارية. من المفترض أن يستخدم مجلد **/usr/local/** من قبل المسؤول لتثبيت التطبيقات يدويًا دون الكتابة فوق الملفات التي يعالجها نظام الحزم (**dpkg**).
/var/	البيانات المتغيرة التي تعالجها الخوادم. يتضمن هذا ملفات السجل، قوائم الانتظار، التخزين المؤقت، وذاكرة التخزين المؤقت. variable
/proc/ and **/sys/**	خاصة بنواة Linux (وليست جزءًا من FHS). يتم استخدامها بواسطة النواة لتصدير البيانات إلى مساحة المستخدم.

٢.٣.٣. مجلد المستخدم الرئيسي

محتويات المجلد الرئيسي للمستخدم غير موحدة ولكن لا تزال هناك بعض المصطلحات الجديرة بالملاحظة. أحدهما هو أن المجلد الرئيسي للمستخدم غالبًا ما يشار إليه بواسطة التلدة ("~"). من المفيد معرفة ذلك لأن مترجمي الأوامر يستبدلون التلدة تلقائيًا بالمجلد الصحيح (الذي يتم تخزينه في متغير بيئة **HOME**، وتكون قيمته المعتادة /**home**/*user*/).

تقليديًا، غالبًا ما يتم تخزين ملفات تكوين التطبيق مباشرةً في مجلدك الرئيسي، ولكن عادةً ما تبدأ أسماء الملفات بنقطة (على سبيل المثال، يخزن عميل البريد الإلكتروني **mutt** تكوينه في **muttrc.**/~). لاحظ أن أسماء الملفات التي تبدأ بنقطة هي مخفية افتراضيًا؛ الأمر **ls** يعرضهن فقط عند استخدام الخيار **a-** ويحتاج مديرو الملفات الرسومية إلى التهيئة بشكل صريح لعرض الملفات المخفية. تستخدم بعض البرامج أيضًا ملفات تكوين متعددة منظمة في مجلد واحد (على سبيل المثال، /**ssh.**/~). تستخدم بعض التطبيقات (مثل متصفح الويب Firefox) مجلدها أيضًا لتخزين ذاكرة التخزين المؤقت للبيانات التي تم تنزيلها. هذا يعني أن تلك المجلدات يمكن أن تستهلك الكثير من مساحة القرص.

ملفات الضبط هذه تخزن مباشرة في مجلدك الرئيسي، والتي يشار إليها مجتمعة في الغالب باسم *dotfiles*، قد انتشرت لفترة طويلة لدرجة أن هذه المجلدات يمكن تشويشها تمامًا. لحسن الحظ، نتج عن جهد بقيادة جماعية تحت مظلة FreeDesktop.org XDG مواصفات المجلدات الأساسية، وهي اتفاقية تهدف إلى تنظيف هذه الملفات والمجلدات. تنص هذه المواصفات على أنه ينبغي تخزين ملفات الضبط أو التكوين في **config.**/~ وملفات ذاكرة التخزين المؤقت في **cache.**/~ وملفات بيانات التطبيق في **local.**/~ (أو المجلدات الفرعية الخاصة بها). هذه الاتفاقية تكتسب شعبيتها ببطء.

تحتوي أسطح المكتب الرسومية عادةً على اختصارات لعرض محتويات مجلد **~/Desktop/** (أو أيا كانت الترجمة المناسبة للأنظمة التي لم تتم تهيئتها باللغة الإنجليزية).

أخيرًا، يقوم نظام البريد الإلكتروني أحيانًا بتخزين رسائل البريد الإلكتروني الواردة في مجلد **~/Mail/**.

٤.٣. أوامر مفيدة

١.٤.٣. عرض وتعديل الملفات النصية

يقوم أمر `cat file` (المقصود به تسلسل(*concatenate*) الملفات لجهاز الإخراج القياسي) بقراءة الملف وعرض محتوياته على الـ(terminal). إذا كان الملف أكبر من أن يتم احتواؤه على الشاشة، فيمكنك استخدام قارء الصفحات مثل **less** (أو **more**) لعرضه صفحة تلو الأخرى.

يبدأ أمر **editor** في تحرر نصوص (مثل **vi** أو **nano**) ويسمح بإنشاء وتعديل وقراءة الملفات النصية. يمكن في بعض الأحيان إنشاء الملفات الأبسط مباشرة من مترجم الأوامر بفضل إعادة التوجيه: *command > file* ينشئ ملفًا باسم ملف يحتوي على مخرجات الأمر المحدد. يشبه *command >> file* إلا أنه يضيف إخراج الأمر في الملف بدلاً من الكتابة فوقه.

$echo "Kali rules!" > kali-rules.txt

$cat kali-rules.txt

Kali rules!

$echo "Kali is the best!" >> kali-rules.txt

$cat kali-rules.txt

Kali rules!

Kali is the best!

٢.٤.٣. البحث عن الملفات وداخل الملفات

يبحث أمر (المعايير) (المجلد) **find** عن الملفات في التسلسل الهرمي ضمن المجلد وفقًا لعدة معايير. المعيار الأكثر استخدامًا هو (اسم الملف) **name-** الذي يسمح بالبحث عن ملف بالاسم. يمكنك أيضًا استخدام أحرف البدل الشائعة مثل "*" في البحث عن اسم الملف.

$find /etc -**name** hosts

/etc/hosts

/etc/avahi/hosts

$find /etc -**name** "hosts"*

/etc/hosts

/etc/hosts.allow

/etc/hosts.deny

/etc/avahi/hosts

يبحث أمر **grep** في محتويات الملفات ويستخرج الأسطر المطابقة للتعبير العادي. تتيح إضافة الخيار **r-** إجراء بحث متكرر على جميع الملفات الموجودة في المجلد. يتيح لك هذا البحث عن ملف عندما تعرف جزءًا فقط من محتوياته.

٣.٤.٣. إدارة العمليات

يسرد أمر **ps aux** قائمة العمليات التي تعمل حاليًا ويساعد على تحديدها من خلال إظهار معرف PID الخاص بهم. بمجرد معرفة PID لعملية ما، يسمح لك الأمر:

kill -*signal pid*

بإرسال إشارة (إذا كنت تملك العملية). توجد عدة اشارات الأكثر استخدامًا هي **TERM** (طلب إنهاء بأمان) و **KILL** (قتل إجباري).

يمكن لمترجم الأوامر أيضًا تشغيل البرامج في الخلفية إذا كان الأمر يتبعه "**&**". باستخدام علامة الضم، تستأنف التحكم في الصدفة فورًا على الرغم من أن الأمر لا يزال قيد التشغيل (مخفي عن المشاهدة كعملية خلفية). يسرد أمر **jobs** العمليات التي تعمل في الخلفية، يؤدي تشغيل:

fg %*job-number* (للمقدمة)

إلى استعادة العملية للمقدمة. عندما يكون هناك أمر قيد التشغيل في المقدمة (إما بسبب بدء تشغيله بشكل طبيعي أو إعادته إلى المقدمة باستخدام **fg**)، فإن مجموعة المفاتيح Control + Z توقف العملية وتستأنف التحكم في سطر الأوامر. يمكن بعد ذلك إعادة تشغيل العملية في الخلفية باستخدام:

bg %*job-number* (للخلفية)

٤.٤.٣. إدارة الحقوق

Linux هو نظام متعدد المستخدمين، لذلك من الضروري توفير نظام أذونات للتحكم في مجموعة العمليات المعتمدة على الملفات والمجلدات، والتي تشمل جميع موارد النظام والأجهزة (على نظام Unix، يتم تمثيل أي جهاز بواسطة ملف أو مجلد). هذا المبدأ شائع في جميع الأنظمة الشبيهة بيونكس.

كل ملف أو مجلد له أذونات محددة لثلاث فئات من المستخدمين:

- ❖ مالكها (يرمز له بـ **u**، اختصار لـ user).
- ❖ مجموعة المالكين (يرمز لهم بـ **g**، اختصار لـgroup)، والتي تمثل جميع أعضاء المجموعة.
- ❖ آخرين (يرمز لهم بـ **o**، اختصار لـ other).

وثلاثة أنواع من الحقوق:

- ❖ القراءة (يرمز لها بـ **r**، اختصار لـ read).
- ❖ الكتابة (أو التعديل، يرمز لها بـ **w**، اختصار لـ write).
- ❖ التنفيذ (يرمز له بـ **x**، اختصار لـ eXecute).

في حالة وجود ملف، يمكن فهم هذه الحقوق بسهولة: يتيح الوصول للقراءة: قراءة المحتوى (بما في ذلك النسخ)، ويسمح الوصول للكتابة: بتغييره، ويسمح الوصول للتنفيذ: بتشغيله (والذي لن يعمل إلا إذا كان برنامجًا).

أمن setuid و setgid التنفيذي

تسمح متغيرات البيئة بتخزين الإعدادات العامة للصدفة أو البرامج الأخرى المختلفة. فهي سياقية ولكن قابلة للتوريث. على سبيل المثال، تحتوي كل عملية على مجموعة متغيرات البيئة الخاصة بها (فهي سياقية). يمكن أن تقوم الصدفات، مثل صدفة تسجيل الدخول، بإعلان المتغيرات، والتي سيتم نقلها إلى البرامج الأخرى التي تنفذها (وهي قابلة للتوريث).

يمكن تعريف هذه المتغيرات على مستوى النظام في etc/profile/ أو لكل مستخدم في ملف التعريف profile./ ~ ولكن يتم وضع المتغيرات غير الخاصة بمترجمي سطر الأوامر بشكل أفضل في etc/environment/، حيث سيتم حقن هذه المتغيرات في جميع المستخدمين جلسات العمل بفضل وحدة المصادقة القابلة للتوصيل (PAM) - حتى في حالة عدم تنفيذ برنامج shell.

هناك نوعان من الحقوق المتعلقة بالملفات القابلة للتنفيذ: **setuid** و**setgid** (يرمز إليها بالحرف "s"). لاحظ أننا نتحدث كثيرًا عن bit، نظراً لأن كل من هذه القيم المنطقية يمكن تمثيلها بالرقم ٠ أو ١. تسمح هذه الحقوق لأي مستخدم بتنفيذ البرنامج بحقوق المالك أو المجموعة، على التوالي. تتيح هذه الآلية الوصول إلى الميزات التي تتطلب أذونات مستوى أعلى من تلك التي عادة ما تكون لديك.

نظراً لأن برنامج الجذر **setuid** يتم تشغيله بشكل منتظم تحت هوية المستخدم الفائق، فمن المهم للغاية التأكد من أنه آمن وموثوق. يمكن لأي مستخدم يدير تخريب برنامج جذر setuid لاستدعاء أمر من اختياره أن ينتحل هوية مستخدم الجذر ويحصل على جميع الحقوق على النظام. يبحث مختبروا الاختراق بشكل منتظم عن هذه الأنواع من الملفات عندما يتمكنون من الوصول إلى النظام كوسيلة لتصعيد امتيازاتهم.

يتم التعامل مع المجلد بشكل مختلف عن الملف. حق الوصول للقراءة يعطي حق الاطلاع على قائمة محتوياته (الملفات والمجلدات)، حق الكتابة يسمح بإنشاء أو حذف الملفات، وحق التنفيذ يسمح بالعبور عبر المجلد للوصول إلى محتوياته (على سبيل المثال، باستخدام الأمر **cd**). أن تكون قادرًا على عبور مجلد دون القدرة على قراءته، يمنح المستخدم إذنًا بالوصول إلى الإدخالات الموجودة فيه والمعروفة بالاسم، ولكن لا يمكن العثور عليها دون معرفة اسمها الدقيق.

أمن مجلد setgid و sticky bit

setgid bit ينطبق أيضًا على المجلدات. أي عنصر تم إنشاؤه حديثًا في مثل هذه المجلدات يتم تلقائيًا تعيين مجموعة المالكين للمجلد الأصل، بدلاً من وراثة المجموعة الرئيسية للمنشئ كالمعتاد. لهذا السبب، لا يتعين عليك تغيير مجموعتك الرئيسية (باستخدام الأمر **newgrp**) عند العمل في شجرة ملفات مشتركة بين عدة مستخدمين لنفس المجموعة المخصصة.

sticky bit (التي يرمز لها بالحرف "**t**") هي إذن مفيد في المجلدات فقط. يستخدم بشكل خاص في المجلدات المؤقتة حيث يكون لكل شخص حق الوصول للكتابة (مثل **/tmp/**): فهو يقيد حذف الملفات بحيث يمكن فقط لمالكها أو مالك المجلد الأصل حذفها. في غياب ذلك، يمكن للجميع حذف ملفات المستخدمين الآخرين في **/tmp/**.

ثلاثة أوامر تتحكم في الأذونات المرتبطة بملف:

```
1.    chown (المستخدم) (الملف)
```

لتغيير صاحب الملف.

> **نصحية لتغيير المستخدم والمجموعة**
>
> كثيرا ما تريد تغيير مجموعة الملف في نفس الوقت الذي تريد تغير المالك فيه. يحتوي الأمر **chown** على بنية خاصة بذلك:
>
> **chown** *user:group file*

لتغيير مجموعة المالكين:

```
2.    chgrp (المجموعة) (الملف)
```

لتغيير أذونات الملف:

```
3.    chmod (الحقوق) (الملف)
```

هناك طريقتان لتمثيل الحقوق، من بينها: **التمثيل الرمزي**: هو على الأرجح أسهل للفهم والتذكر. أنه يتكون من رموز الحروف المذكورة أعلاه. يمكنك تحديد الحقوق لكل فئة من فئات المستخدمين (**u / g / o**)، عن طريق تعيينها بشكل صريح (بـ =)، أو عن طريق إضافة (+)، أو طرح (-). وبالتالي فإن صيغة **u=rwx,g+rw,o-r**، تمنح المالك حقوق القراءة والكتابة والتنفيذ، وتضيف حقوق القراءة والكتابة لمجموعة المالكين، وتزيل حقوق القراءة للمستخدمين الآخرين. الحقوق التي لا تتغير عن طريق الجمع أو الطرح في مثل هذا الأمر تبقى غير معدلة. يعطي الحرف **a**، لجميع فئات المستخدمين الثلاثة، مثال: **a=rx** يمنح الفئات الثلاث نفس الحقوق (القراءة والتنفيذ، لكن ليس الكتابة).

يربط التمثيل الرقمي (الثماني) كل حق بقيمة:

- ❖ ٤: للقراءة.
- ❖ ٢: للكتابة.
- ❖ ١: للتنفيذ.

نحن نربط كل مجموعة من الحقوق بمجموع الأرقام الثلاثة، ويتم تعيين قيمة لكل فئة من فئات المستخدمين، بالترتيب المعتاد (المالك، المجموعة، آخرون).

على سبيل المثال، سيضع أمر *(الملف)* **chmod 754** الحقوق التالية: القراءة والكتابة والتنفيذ للمالك (حيث ٧=٤+٢+١)؛ القراءة والتنفيذ للمجموعة (حيث ٥=٤+١)؛ والآخرين القراءة فقط. الصفر 0 يعني عدم وجود حقوق؛ وبالتالي يسمح *(ملف)* **chmod 600** لأذونات القراءة والكتابة للمالك، ولا حقوق لأي شخص آخر. المجموعات الصحيحة الأكثر شيوعًا هي **755** للملفات القابلة للتنفيذ والمجلدات، و 644 لملفات البيانات.

لتمثيل الحقوق الخاصة، يمكنك اختصار أربعة أرقام لهذا الرقم وفقًا لنفس المبدأ، حيث تكون وحدات البت **setuid** و**setgid** و **sticky** هي ٤ و ٢ و ١ على التوالي. سيقوم الأمر **chmod 4754** بربط setuid bit مع الحقوق الموصوفة مسبقًا.

لاحظ أن استخدام الترميز الثماني يسمح لك فقط بتعيين جميع الحقوق في ملف واحد؛ **لا يمكنك استخدامه لإضافة حق جديد،** مثل الوصول للقراءة لمالك المجموعة، حيث يجب أن تأخذ في الاعتبار الحقوق الحالية وحساب القيمة العددية الجديدة المقابلة.

يتم استخدام التمثيل الثماني أيضًا مع أمر **umask**، والذي يُستخدم لتقييد الأذونات على الملفات التي تم إنشاؤها حديثًا. عندما يقوم أحد التطبيقات بإنشاء ملف، فإنه يعين أذونات إرشادية، مع العلم أن النظام يزيل تلقائيًا الحقوق المحددة باستخدام **umask**. اكتب **umask** في الصدفة.

سترى قناعًا مثل **0022**. هذا مجرد تمثيل ثماني للحقوق المراد إزالتها بشكل منهجي (في هذه الحالة، حقوق الكتابة للمجموعة والمستخدمين الآخرين).

إذا أعطيتها قيمة ثمانية جديدة، فإن أمر **umask** يعدل القناع. المستخدمة في ملف تهيئة الصدفة (على سبيل المثال، **bash_profile./~**) ، سيغير القناع الافتراضي لجلسات عملك بشكل فعال.

نصحية للعمليات مكررة

أحيانا، يتعين علينا تغيير الحقوق لشجرة الملفات بالكامل. جميع الأوامر المذكورة أعلاه لها خيار **R-** للعمل بشكل متكرر في المجلدات الفرعية.

يؤدي التمييز بين المجلدات والملفات أحيانًا إلى حدوث مشكلات في العمليات المتكررة. لهذا السبب تم تقديم حرف "**X**" في التمثيل الرمزي للحقوق. إنه يمثل حق التنفيذ الذي ينطبق فقط على المجلدات (وليس على الملفات التي تفتقر إلى هذا الحق). وبالتالي، فإن:

```
chmod -R a+X المجلد
```

سيضيف فقط حقوق التنفيذ لجميع فئات المستخدمين (a) لجميع المجلدات الفرعية والملفات التي لديها بالفعل فئة واحدة على الأقل من المستخدمين (حتى لو كان مالكها الوحيد) لديها حقوق تنفيذ .

٥.٤.٣. الحصول على معلومات النظام والسجلات

يعرض الأمر **free** معلومات عن الذاكرة العشوائية (RAM).

free disk (**df**): يعطي تقارير عن مساحة القرص المتوفرة على كل من الأقراص المثبتة في نظام الملفات. الخيار **h-** (للقراءة البشرية (*human readable*)) يحول الأحجام إلى وحدة أكثر وضوحًا (عادةً mebibytes أو gibibytes). بطريقة مماثلة، يدعم الأمر **free** خيارات **m-** و **g-**، ويعرض بياناته إما بـ mebibytes أو بـ gibibytes، على التوالي.

```
$free
              total        used        free      shared  buff/cache
available
Mem:        2052944      661232      621208       10520      770504
1359916
Swap:             0           0           0
$df
Filesystem     1K-blocks     Used Available Use% Mounted on
udev             1014584        0   1014584   0% /dev
tmpfs             205296     8940    196356   5% /run
/dev/vda1       30830588 11168116  18073328  39%/
tmpfs            1026472      456   1026016   1% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs            1026472        0   1026472   0% /sys/fs/cgroup
tmpfs             205296       36    205260   1% /run/user/132
tmpfs             205296       24    205272   1% /run/user/0
```

يعرض الأمر **id** هوية المستخدم الذي يدير الجلسة مع قائمة المجموعات التي ينتمي لها. نظراً لأن الوصول إلى بعض الملفات أو الأجهزة قد يقتصر على أعضاء المجموعة، فقد يكون التحقق من عضوية المجموعة المتاحة مفيدًا.

```
$ id
uid=1000(buxy) gid=1000(buxy) groups=1000(buxy),27(sudo)
```

يُرجع الأمر **uname -a** سطراً واحدًا يوثق اسم النواة (**linux**) واسم المضيف وإطلاق النواة وإصدار النواة ونوع الجهاز (والبنية، مثل: **x86_64**) واسم نظام التشغيل (**GNU/Linux**). عادةً ما يجب تضمين إخراج هذا الأمر في تقارير الأخطاء حيث إنه يحدد بوضوح النواة قيد الاستخدام ومنصة الأجهزة التي تعمل عليها.

```
$ uname -a
Linux kali-rolling 4.4.0-kali1-amd64 #1 SMP Debian 4.4.6-1kali1 (2016-03-18)
x86_64 GNU/Linux
```

توفر كل هذه الأوامر معلومات حول وقت التشغيل، ولكن غالبًا ما تحتاج إلى التحقق من السجلات لفهم ما حدث على جهازك. على وجه الخصوص، النواة تبعث الرسائل التي تخزنها في المخزن المؤقت الحلقي كلما حدث شيء مثير للاهتمام (مثل إدخال جهاز USB جديد، أو فشل تشغيل القرص الصلب، أو الكشف الأولي عن الأجهزة عند الإقلاع). يمكنك استرداد سجلات النواة باستخدام الأمر **dmesg**.

تقوم مجلة Systemd أيضًا بتخزين سجلات متعددة (مخرجات stdout/stderr من daemons، رسائل syslog، سجلات النواة) وتجعل من السهل طلبها باستخدام **journalctl**. بدون أي معلمات، فإنه يقوم فقط بعرض جميع السجلات المتاحة بطريقة التسلسل الزمني. باستخدام الخيار **r**- سيعكس الترتيب بحيث تظهر الرسائل الأحدث أولاً. باستخدام الخيار **f**- سوف يطبع إدخالات السجل الجديد باستمرار حيث يتم إلحاقها بقاعدة البيانات الخاصة به. يمكن لخيار **u**- قصر الرسائل على تلك التي تنبعث من وحدة نظام معينة (على سبيل المثال:

journalctl -u ssh.service).

٦.٤.٣. استكشاف الهاردوير

تقوم النواة بتصدير العديد من التفاصيل حول الأجهزة المكتشفة من خلال نظام الملفات **/proc/** و **/sys/** الافتراضي. هناك عدة أدوات تلخص تلك التفاصيل. فيما بينها، يسرد **lspci** (في الحزمة pciutils) أجهزة PCI، ويسرد **lsusb** (في الحزمة usbutils) أجهزة USB، ويسرد **lspcmcia** (في الحزمة pcmciautils) بطاقات PCMCIA. هذه الأدوات مفيدة للغاية لتحديد النموذج الدقيق للجهاز. يتيح هذا التعريف أيضًا إجراء عمليات بحث أكثر دقة على الويب، مما يؤدي بدوره إلى المزيد من المستندات ذات الصلة. لاحظ أن حزم pciutils و usbutils مثبتة بالفعل على نظام Kali الأساسي ولكن يجب تثبيت pcmciautils بكتابة الأمر:

```
apt install pcmciautils
```

سنناقش المزيد حول تثبيت الحزم وإدارتها في فصل لاحق.

مثال ٣.١. مثال على المعلومات المخرجة من **lspci** و **lsusb**

```
$ lspci
[...]
00:02.1 Display controller: Intel Corporation Mobile 915GM/GMS/910GML Express
Graphics Controller (rev 03)
00:1c.0 PCI bridge: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) PCI
Express Port 1 (rev 03)
00:1d.0 USB Controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family)
USB UHCI #1 (rev 03)
[...]
01:00.0 Ethernet controller: Broadcom Corporation NetXtreme BCM5751 Gigabit
 Ethernet PCI Express (rev 01)
02:03.0 Network controller: Intel Corporation PRO/Wireless 2200BG Network
Connection (rev 05)
$ lsusb
Bus 005 Device 004: ID 413c:a005 Dell Computer Corp.
Bus 005 Device 008: ID 413c:9001 Dell Computer Corp.
Bus 005 Device 007: ID 045e:00dd Microsoft Corp.
Bus 005 Device 006: ID 046d:c03d Logitech, Inc.
[...]
Bus 002 Device 004: ID 413c:8103 Dell Computer Corp. Wireless 350 Bluetooth
```

تحتوي هذه البرامج على خيار **v-** يسرد معلومات أكثر تفصيلاً (لكنها عادةً غير ضرورية). أخيرًا، يسرد الأمر **lsdev** (في الحزمة procinfo) موارد الاتصال المستخدمة بواسطة الأجهزة.

برنامج **lshw** هو مزيج من البرامج المذكورة أعلاه ويعرض وصفًا طويلًا للأجهزة المكتشفة بطريقة هرمية. يجب إرفاق الإخراج الكامل لأي تقرير حول مشاكل دعم الأجهزة.

٥.٣. ملخص

في هذا الفصل، قمنا بجولة حول طبيعة Linux. ناقشنا مساحة النواة والمستخدم، واستعرضنا العديد من أوامر صدفة لينكس الشائعة، وناقشنا العمليات وكيفية إدارتها، واستعرضنا مفاهيم أمان المستخدم والمجموعة، وناقشنا نظام الملفات الهرمي FHS، وقمنا بجولة في بعض المجلدات والملفات الأكثر شيوعًا الموجودة في Kali Linux.

نصائح التلخيص:

غالبًا ما يتم استخدام Linux للإشارة إلى نظام تشغيل بالكامل، ولكن في الواقع لينكس هو نواة نظام التشغيل الذي يتم تشغيله بواسطة أداة محمل الإقلاع، والتي يتم تشغيلها هي نفسها بواسطة BIOS / UEFI.

تشير مساحة المستخدم إلى كل ما يحدث خارج النواة. من بين البرامج التي يتم تشغيلها في مساحة المستخدم، هناك العديد من الأدوات المساعدة الأساسية من مشروع GNU، ومعظمها يهدف إلى تشغيلها من سطر الأوامر (واجهة قائمة على النصوص تتيح لك إدخال الأوامر وتنفيذها، وعرض النتائج). تنفذ الصدفة الأوامر الخاصة بك داخل تلك الواجهة.

تتضمن الأوامر الشائعة:

- ❖ **pwd** (print working directory).
- ❖ **cd** (change directory).
- ❖ **ls** (listing).

- ❖ **mkdir** (make directory).
- ❖ **rmdir** (remove directory).
- ❖ **mv**، **rm** ، و **cp** (move, remove and copy).
- ❖ **cat** (concatenate).
- ❖ **more/less** (عرض الملفات صفحة تلو الأخرى).
- ❖ **editor** (بدء تشغيل محرر نصي).
- ❖ **find** (تحديد موقع ملف أو مجلد).
- ❖ **free** (عرض معلومات الذاكرة).
- ❖ **df** (disk free).
- ❖ **id** هوية المستخدم إلى جانب قائمة المجموعات التي ينتمي لها.
- ❖ **dmesg** (مراجعة سجلات النواة).
- ❖ **journalctl** (إظهار جميع السجلات المتاحة).

يمكنك التفاعل مع الجهاز على نظام Kali باستخدام العديد من الأوامر:

- ❖ **lspci** (قائمة أجهزة PCI).
- ❖ **lsusb** (قائمة أجهزة USB).
- ❖ **lspcmcia** (تسرد بطاقات PCMCIA).

العملية عبارة عن مثيل قيد التشغيل لبرنامج، والذي يتطلب ذاكرة لتخزين كل من البرنامج نفسه وبيانات التشغيل الخاصة به. يمكنك إدارة العمليات باستخدام أوامر مثل:

- ❖ **ps** (show processes).
- ❖ **kill** (kill processes).
- ❖ **bg** (send process to background).
- ❖ **fg** (bring background process to foreground).
- ❖ **jobs** (show background processes).

الأنظمة التي تشبه يونيكس متعددة المستخدمين. تدعم العديد من المستخدمين والمجموعات وتسمح بالتحكم في الإجراءات، بناءً على الأذونات. يمكنك إدارة حقوق الملفات والمجلدات باستخدام العديد من الأوامر، بما في ذلك:

- ❖ **chmod** (تغيير الأذونات).
- ❖ **chown** (تغيير المالك).
- ❖ **chgrp** (تغيير المجموعة).

كما هو الحال مع توزيعات Linux الأخرى، تم تنظيم Kali Linux بحيث يكون متوافقًا مع معيار نظام الملفات الهرمي (FHS)، مما يسمح للمستخدمين القادمين من توزيعات Linux الأخرى بالعثور على مساراتهم بسهولة في Kali.

بشكل تقليدي، يتم تخزين ملفات تكوين التطبيق ضمن مجلدك الرئيسي (home)، الملفات أو المجلدات المخفية تبدأ بنقطة.

الآن بعد أن أصبح لديك فكرة على أساسيات Linux، فلنقم بإنشاء Kali Linux وتشغيله.

التمرين الأول للفصل الثالث

١. استخدم الأمر **`file`** لفحص بعض الأجهزة التي تم تصديرها بواسطة النواة في /dev/.
جرب **/dev/sda*** و **/dev/snd/***.

يرجى ملاحظة أنه إذا كنت تواجه مشكلة في الأوامر والمفاهيم الأساسية لنظام Linux، فيجب عليك التفكير بجدية في الحصول على دورة تدريبية مجانية على نظام Linux (مثل هذه الدورة التدريبية) قبل مواصلة تدريب Kali. تذكر! Kali Linux ليست لمبتدئي Linux!

التمرين الثاني للفصل الثالث: التحكم في العلميات

١. اكتب الأمر:

```
ping -i 10 localhost &
```

٢. بعدها، أكتب الأمر:

```
ping -i 10 127.0.0.1 &
```

٣. اعرض قائمة العلميات التي في الخلفية.

٤. انهِ عملية localhost

٥. الأن، أنهِ عملية ١,٠,٠,١٢٧

الإجابة:

يجب أن يكون الأمر كالاتي:

```
root@kali:~# ping -i 10 localhost &
[1] 3605
root@kali:~#  ping -i 10 127.0.0.1 &
[2] 3606
root@kali:~# jobs -l
[1]-  3605 Running                 ping -i 10 localhost &
[2]+  3606 Running                 ping -i 10 127.0.0.1 &
root@kali:~# kill %1
root@kali:~# jobs -l
[1]-  3605 Terminated              ping -i 10 localhost
[2]+  3606 Running                 ping -i 10 127.0.0.1 &
oot@kali:~# kill %2
root@kali:~# jobs -l
[2]+  3606 Terminated              ping -i 10 127.0.0.1
root@kali:~#
```

التمرين الثالث للفصل الثالث: البحث في وعن الملفات

١. جرب الأمر **dmesg** الذي يطبع رسائل النواة المخزنة، يحتوي إخراج هذا الأمر عادة على الرسائل التي تنتجها برامج تشغيل الأجهزة.

٢. استخدم الأمر **find** للعثور على ملف مسمى rockyou.txt.gz في نظام الملفات.

٣. استخدم الأمر **locate** لإيجاد ملف يسمى rockyou.txt.gz في نظام الملفات.

٤. أي أمر كان أسرع في البحث `find` أو `locate`، ولماذا؟

٥. يمكنك معرفة كيفية "الوقت" الأوامر لمعرفة مقدار الوقت الفعلي الذي تستغرقه الأوامر لإكمال؟

الإجابات:

١. إنه سهل جدا

```
dmesg | more
```

٢. أمر **find**:

```
find / -name rockyou.txt.gz
```

٣. أمر **locate**:

```
locate rockyou.txt.gz
```

٤. يجب أن يستغرق الأمر "**locate**" وقتًا أقل، بدلاً من البحث في نظام الملفات بالكامل عن ملف معين، يبحث الأمر "**locate**" في قاعدة بيانات تم تجميعها مسبقًا للملف المطلوب. في حال كنت تتساءل، يتم إنشاء قاعدة البيانات هذه كجزء من Kali ISO build، باستخدام الأمر "**updateb**". يمكنك استخدام الملف، ثم **zcat** لمعالجة هذا الملف.

٥. استخدم أمر **time** ^^!

التمرين الرابع للفصل الثالث: استكشاف الهاردوير

استخدام **`lspci`** و **`dmesg`** وأي أدوات مساعدة أخرى للتسجيل، اكتشف ما يلي حول مضيف Kali الخاص بك:

١. نوع وحدة المعالجة المركزية على مضيف Kali الخاص بك.

٢. نوع، وصنع وطراز محول إيثرنت.

٣. نوع وصنع ونموذج بطاقة الرسومات.

٤. نسخة من نواة قيد التشغيل.

٥. ذاكرة متاحة.

٦. مساحة القرص الحرة.

الإجابة:

1. **dmesg** | **grep** CPU0
2. **lspci** | **grep** Ethernet
3. **lspci -v -s** `lspci | **grep** VGA | cut -f1 -d\ `
4. **uname** –**r**
5. **free**
6. **df**

التمرين الخامس للفصل الثالث: العمل على الهاردوير

١. قم بتوصيل أي جهاز USB بنظام الـ Kali الخاص بك.

٢. اعرف اسم هذا الجهاز.

٣. قم بتوصيل بطاقة USB لاسلكية بنظام الـ Kali.

٤. اعرف شرائح وطراز البطاقة اللاسلكية.

الإجابة:

انظر لمخرجات **lsusb** و **dmesg**.

غذاء الفكر:

١. ما نوع جهاز dev/urandom/؟

٢. أين يمكنني إيجاد ملفات ضبط الخوادم؟

الإجابة:

1. A character device: **ls -l /dev/random**

/* هذه الإجابة من الموقع، أما أنا كتبت file /dev/urandom */

2. /etc/

اختبار الشهادة للفصل الثالث

١. ما هو الحرف المستخدم لتمثيل المجلد الرئيسي للمستخدم؟

- ☐ ~
- ☐ !
- ☐ ?
- ☐ &

٢. ما هي الأدوات التي يمكن استخدامها للحصول على معلومات الملف؟ اختار كل ما ينطبق.

- ☐ pwd
- ☐ type
- ☐ echo
- ☐ which
- ☐ cat

٣. أي مما يلي ليس جهاز كتلة ولا حرف؟

- ☐ crw-rw—- 1 root tty 7, 132 Mar 21 08:30 vcsa4
- ☐ crw——- 1 root root 10, 63 Mar 21 08:30 vga_arbiter
- ☐ brw-rw—- 1 root disk 8, 0 Mar 21 08:30 sda
- ☐ drwxr-xr-x 2 root root 60 Mar 21 08:30 vfio

٤. كيف يمكن تمثيل أذونات الملف -r —w- بالرمز الثماني؟

- ☐ 751
- ☐ 420
- ☐ 411
- ☐ 110
- ☐ 200

٥. بناءً على قائمة الدليل الجزئي التالية، ما هي أذونات المستخدم لملف test؟

-r-x--x--- 1 user root 0 Mar 24 01:19 test

- ☐ بدون أذونات
- ☐ Read, Write, Execute
- ☐ Read, Execute
- ☐ Execute

٦. لديك وظيفتان تعملان في الخلفية. كيف تنهي أول وظيفة نفذتها؟

- ☐ CTRL-C
- ☐ `kill %1`
- ☐ `killall`
- ☐ `kill -signal pid`

٠٧ أي أمر لا يتحكم في الأذونات أو سمات المستخدم المرتبطة بالملف؟

- ☐ chperm
- ☐ chgrp
- ☐ chmod
- ☐ chown

٠٨ أي أمر يعرض هوية المستخدم الذي يدير الجلسة مع قائمة المجموعات التي ينتمي لها؟

- ☐ cat /etc/passwd
- ☐ id
- ☐ who
- ☐ whoami

٠٩ أي أمر يلخص أجهزة PCI من خلال أنظمة الملفات الافتراضية proc/ و sys/؟

- ☐ pci -v
- ☐ cat /proc/pci
- ☐ pciutil
- ☐ lspci

١٠. وفقًا لـ FHS، ما المجلد الذي يحتوي على ملفات السجل، وقوائم الانتظار، وملفات التخزين المؤقت، وبيانات ذاكرة التخزين المؤقت التي تتعامل معها ||الخوادم|| daemons؟

- ☐ /proc
- ☐ /var
- ☐ /sbin
- ☐ /bin

-----((الفصل الرابع))-----

تثبيت Kali Linux

في هذا الفصل، سوف نركز على عملية تثبيت Kali Linux. أولاً، سنناقش الحد الأدنى لمتطلبات التثبيت (الباب ١.٤. "الحد الأدنى لمتطلبات التثبيت") للتأكد من أن نظامك الحقيقي أو الافتراضي قد تم تهيئته بشكل جيد للتعامل مع نوع التثبيت الذي ستتبعه. بعد ذلك، سوف نمر بكل خطوة من خطوات عملية التثبيت (الباب ٢.٤. "التثبيت خطوة بخطوة على القرص الصلب") للتثبيت العادي، وكذلك للتثبيت الأكثر أمانًا الذي يتضمن نظام ملفات مشفر بالكامل.

سوف نناقش أيضًا مرحلة ما *قبل التثبيت* "preseeding"، والتي تسمح بالتثبيتات غير المراقبة (الباب ٣.٤. "التثبيتات الغير مراقبة") من خلال تقديم إجابات محددة مسبقًا على أسئلة التثبيت. سنبين لك أيضًا كيفية تثبيت Kali Linux على أجهزة ARM المختلفة (الباب ٤.٤. "تثبيتات ARM")، مما يوسع قدرات Kali إلى أبعد من سطح مكتب. أخيرًا، سوف نوضح لك ما يجب القيام به في حالة نادرة فشل التثبيت (الباب ٥.٤. "استكشاف أخطاء التثبيتات")، حتى تتمكن من حل المشكلة وإنهاء عملية تثبيت صعبة بنجاح.

١.٤. الحد الأدنى لمتطلبات التثبيت

تختلف متطلبات التثبيت لـ Kali Linux حسب ما تريد تثبيته. **الحد الأدنى**، يمكنك إعداد Kali كخادم Secure Shell (SSH) أساسي بدون سطح مكتب، باستخدام ذاكرة وصول عشوائي (RAM) لا تقل عن 128 MB (يوصى باستخدام 512 MB) و2 GB من مساحة القرص. **الحد الأعلى**، إذا اخترت تثبيت سطح مكتب GNOME الافتراضي وحزمة التعريف kali-linux-full، فيجب أن تحصل على 2048 MB على الأقل من ذاكرة الوصول العشوائي و20 GB من مساحة القرص.

إلى جانب متطلبات ذاكرة الوصول العشوائي والأقراص الصلبة، يحتاج الحاسوب لديك إلى وحدة المعالجة المركزية مدعومة على الأقل من بنيات amd64 أو i386 أو armel أو armhf أو arm64.

٢.٤. التثبيت خطوة بخطوة على القرص الصلب

في هذا الباب، نفترض أن لديك محرك أقراص USB أو قرص DVD قابلًا للإقلاع (راجع الباب ٤.١.٢. "نسخ الصورة على قرص DVD-ROM أو مفتاح USB" للحصول على تفاصيل حول كيفية إعداد محرك الأقراص هذا) وأنك قمت بالإقلاع منه لبدء عملية التثبيت.

١.٢.٤. تثبيت عادي

أولاً، سوف نلقي نظرة على تثبيت Kali القياسي، باستخدام نظام ملفات غير مشفر.

١.١.٢.٤. إقلاع وبدء التثبيت

بمجرد بدء BIOS في التشغيل من محرك أقراص USB أو DVD-ROM، تظهر قائمة أداة محمل الإقلاع لصورة لينكس، كما هو مبين في الشكل ١.٤. "شاشة الإقلاع". في هذه المرحلة، لم يتم تحميل نواة لينكس بعد؛ تتيح لك هذه القائمة اختيار نواة للإقلاع وإدخال معلمات اختيارية لنقلها إليه في هذه العملية.

للتثبيت القياسي، ما عليك سوى اختيار install أو Graphical Install (بمفاتيح الأسهم)، ثم اضغط على مفتاح **Enter** لبدء ما تبقى من عملية التثبيت.

يخفي كل إدخال قائمة سطر أوامر إقلاع محددًا، والذي يمكن تهيئته حسب الحاجة عن طريق الضغط على مفتاح **Tab** قبل التحقق من الإدخال والتشغيل.



شكل ١.٤. شاشة الإقلاع

بمجرد الإقلاع، يرشدك برنامج التثبيت خطوة بخطوة خلال العملية. سوف نلقي نظرة على كل خطوة من هذه الخطوات بالتفصيل. سنغطي التثبيت من Kali Linux DVD-ROM قياسي؛ المثبتة من **mini.iso** قد تبدو مختلفة بعض الشيء. سنقوم أيضًا بتثبيت الوضع الرسومي، ولكن الفرق الوحيد من تثبيت وضع النص هو المظهر القديم.

٢.١.٢.٤. اختيار اللغة

كما هو مبين في الشكل ٢.٤ "اختيار اللغة"، يبدأ برنامج التثبيت باللغة الإنجليزية ولكن الخطوة الأولى تسمح لك باختيار اللغة التي سيتم استخدامها لبقية عملية التثبيت. يتم استخدام اختيار اللغة هذا أيضًا لتحديد الخيارات الافتراضية ذات الصلة في المراحل اللاحقة (لا سيما تخطيط لوحة المفاتيح).

التنقل باستخدام لوحة المفاتيح

تتطلب بعض الخطوات في عملية التثبيت إدخال المعلومات. تحتوي هذه الشاشات على العديد من الخانات التي تريد الإنتقال لها (خانة إدخال النص، وخانات الاختيار، وقائمة الخيارات، وأزرار الموافقة والإلغاء)، يسمح لك مفتاح **Tab** بالانتقال من خانة لإخرى. في وضع التثبيت الرسومي، يمكنك استخدام الماوس كما تفعل عادةً في سطح مكتب رسومي.



شكل ٢.٤. اختيار اللغة

٣.١.٢.٤. اختيار البلد

تمثل الخطوة الثانية (الشكل ٣.٤. "اختيار البلد") في اختيار بلدك. بالإضافة إلى اللغة، تُمكّن هذه المعلومات برنامج التثبيت من تقديم تخطيط لوحة المفاتيح الأكثر ملاءمة. سيؤثر هذا أيضًا على تكوين المنطقة الزمنية. في الولايات المتحدة، تُقترح لوحة مفاتيح QWERTY قياسية ويقدم المثبت اختيارًا للمناطق الزمنية المناسبة.

KALI
BY OFFENSIVE SECURITY

Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

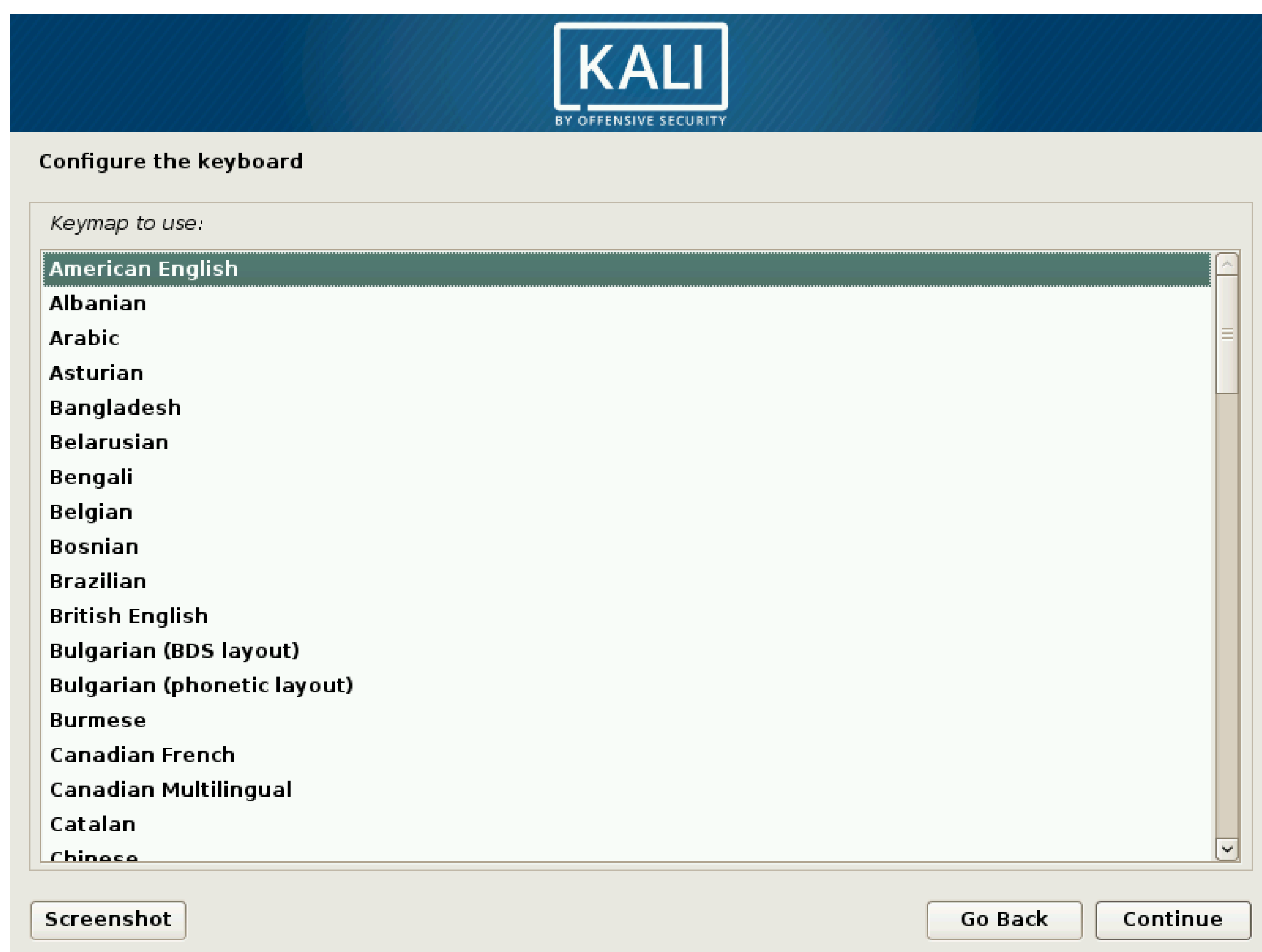
Hong Kong
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

Screenshot | Go Back | Continue

شكل ٣.٤. اختيار البلد

٤.١.٢.٤. اختيار تخطيط لوحة المفاتيح

تتوافق لوحة المفاتيح الإنجليزية الأمريكية المقترحة مع تخطيط QWERTY المعتاد كما هو موضح في الشكل ٤.٤. "اختيار تخطيط لوحة المفاتيح".



شكل ٤.٤. اختيار تخطيط لوحة المفاتيح

٤.٢.١.٥. التعرف على الهاردوير

غالبا تكون خطوة اكتشاف الأجهزة تلقائية بالكامل. يكشف المثبت عن أجهزتك ويحاول تحديد جهاز الإقلاع المستخدم للوصول إلى محتواه. يقوم بتحميل الوحدات المقابلة لمكونات الأجهزة المختلفة المكتشفة، ثم يقوم بوصل جهاز الإقلاع من أجل قراءته. تم تضمين الخطوات السابقة بالكامل في صورة الإقلاع المضمنة في جهاز الإقلاع، وهو ملف ذو حجم محدود ويتم تحميله في الذاكرة بواسطة أداة محمل الإقلاع عند التشغيل من جهاز الإقلاع.

٤.٢.١.٦. تحميل المكونات

مع توفر محتويات جهاز الإقلاع الآن، يقوم المثبت بتحميل جميع الملفات اللازمة لمتابعة عمله. يتضمن ذلك برامج تشغيل إضافية للأجهزة المتبقية (خاصة بطاقة الشبكة)، بالإضافة إلى جميع مكونات برنامج التثبيت.

٤.٢.١.٧. التحقق من هاردوير الشبكة

في هذه الخطوة، سيحاول المثبت تحديد بطاقة الشبكة تلقائيًا وتحميل الوحدة النمطية المقابلة. في حالة فشل الاكتشاف التلقائي، يمكنك تحديد الوحدة النمطية المراد تحميلها يدويًا. إذا فشل كل شيء آخر، يمكنك تحميل وحدة نمطية معينة من جهاز قابل للإزالة. عادة ما تكون هناك حاجة إلى هذا الحل الأخير فقط إذا لم يتم تضمين برنامج التشغيل المناسب في نواة لينكس القياسية، ولكنه متوفر في مكان آخر، مثل موقع الشركة المصنعة على الويب.

يجب أن تكون هذه الخطوة ناجحة تمامًا لعمليات تثبيت الشبكة (مثل تلك التي تمت عند التشغيل من **mini.iso**)، حيث يجب تحميل حزم دبيان من الشبكة.

٨.١.٢.٤ تكوين الشبكة

من أجل أتمتة العملية إلى أقصى حد ممكن، يحاول المثبت تكوين شبكة تلقائي باستخدام بروتوكول تكوين المضيف الحيوي "dynamic host configuration protocol" (DHCP) (لـ IPv4 و IPv6) (for IPv6) and ICMPv6’s Neighbor Discovery Protocol ، كما هو مبين في الشكل ٤.٥. "التكوين التلقائي للشبكة ".



شكل ٤.٥. التكوين التلقائي للشبكة

في حالة فشل التكوين التلقائي، يقدم برنامج التثبيت المزيد من الخيارات: حاول مرة أخرى باستخدام تكوين DHCP عادي، أو حاول تكوين DHCP بالإعلان عن اسم الجهاز، أو قم بإعداد تكوين شبكة ثابت. يتطلب هذا الخيار الأخير عنوان IP وقناع شبكة فرعية وعنوان IP للبوابة واسم الجهاز واسم المجال.

التكوين بدون DHCP

إذا كانت الشبكة المحلية مجهزة بخادم DHCP الذي لا ترغب في استخدامه لأنك تفضل تحديد عنوان IP ثابت للجهاز أثناء التثبيت، يمكنك إضافة خيار **netcfg/use_dhcp=false** عند التشغيل. تحتاج فقط إلى تحرير إدخال القائمة المطلوبة عن طريق الضغط على مفتاح **Tab** وإضافة الخيار المطلوب قبل الضغط على مفتاح **Enter**.

٩.١.٢.٤. كلمة السر للمستخدم الجذر

يطلب المثبت كلمة مرور (الشكل ٦.٤) لأنه يقوم تلقائيًا بإنشاء حساب جذر للمستخدم الفائق.
يطلب المثبت أيضًا تأكيد كلمة المرور لمنع أي خطأ في الإدخال يصعب ضبطه لاحقًا.

KALI
BY OFFENSIVE SECURITY
Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it.
Root password:
Show Password in Clear
Please enter the same root password again to verify that you have typed it correctly.
Re-enter password to verify:
Show Password in Clear
Screenshot
Go Back
Continue

شكل ٦.٤. كلمة مرور المستخدم الجذر

كلمة مرور المسؤول

يجب أن تكون كلمة مرور المستخدم الجذر طويلة (ثمانية أحرف أو أكثر) ولا يمكن تخمينها، لأن المهاجمين يستهدفون أجهزة الحاسوب والخوادم المتصلة بالإنترنت باستخدام أدوات آلية، ومحاولة تسجيل الدخول بكلمات مرور واضحة. يستفيد المهاجمون أحيانًا هجمات القاموس، وذلك باستخدام العديد من مجموعات الكلمات والأرقام وكلمات مرور. تجنب استخدام أسماء الأطفال أو الوالدين وتواريخ الميلاد، لأن هذه يسهل تخمينها.

تنطبق هذه الملاحظات بالتساوي على كلمات مرور المستخدمين الأخرين، لكن عواقب حساب مخترق تكون أقل حدة للمستخدمين دون حقوق إدارية.

إذا كنت تفتقر إلى الإلهام، فلا تتردد في استخدام مولد كلمات المرور، مثل **pwgen** (الموجود في الحزمة التي تحمل الاسم نفسه، والمضمنة بالفعل في تثبيت Kali الأساسي).

٤.٢.١.١٠. تكوين الساعة

إذا كانت الشبكة متوفرة، سيتم تحديث الساعة الداخلية للنظام من خادم بروتوكول وقت الشبكة (NTP). يعد هذا مفيدًا لأنه يضمن أن الطوابع الزمنية على السجلات ستكون صحيحة من الإقلاع الأول.

إذا امتد بلدك إلى مناطق زمنية متعددة، فسيُطلب منك تحديد المنطقة الزمنية التي تريد استخدامها، كما هو موضح في الشكل ٧.٤ "تحديد المنطقة الزمنية".

KALI
BY OFFENSIVE SECURITY

Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa

Screenshot | Go Back | Continue

شكل ٧.٤. تحديد المنطقة الزمنية

٤.٢.١.١١. اكتشاف الأقراص والأجهزة الأخرى

تكتشف هذه الخطوة تلقائيًا محركات الأقراص الثابتة التي يمكن تثبيت Kali عليها، وسيتم تقديم كل منها في الخطوة التالية: التقسيم (partitioning).

٤.٢.١.١٢. التقسيم

التقسيم هو خطوة لا غنى عنها في التثبيت، والتي تتكون من تقسيم المساحة المتوفرة على محركات الأقراص الصلبة إلى أقسام منفصلة (*partitions*) وفقًا للوظيفة المقصودة للحاسوب وتلك الأقسام. يتضمن التقسيم أيضًا اختيار أنظمة الملفات المراد استخدامها. جميع هذه القرارات سيكون لها تأثير على الأداء، وأمن البيانات، وإدارة الخادم.

تعتبر خطوة التقسيم صعبة تقليدياً للمستخدمين الجدد. ومع ذلك، يجب تعريف أنظمة ملفات Linux والأقسام، بما في ذلك الذاكرة الافتراضية (أو أقسام المبادلة) لأنها تشكل أساس النظام. يمكن أن تصبح هذه المهمة معقدة إذا كنت قد قمت بالفعل بتثبيت نظام تشغيل آخر على الجهاز وتريد الحفاظ عليهما الاثنان. في هذه الحالة، يجب عليك التأكد من عدم تغيير أقسامهم، أو تغيير حجمهم إذا لزم الأمر دون التسبب في ضرر.

لفهم أوضاع التقسيم الأكثر شيوعًا (والأكثر بساطة)، يفضل معظم المستخدمين وضع الإرشاد *"Guided"* الذي يوصي بتكوينات القسم ويقدم اقتراحات في كل خطوة في الطريق. سيقدر المستخدمون الأكثر تقدماً الوضع اليدوي *"Manual"*، الذي يسمح بمزيد من التكوينات المتقدمة. يشارك كل وضع بعض القدرات.

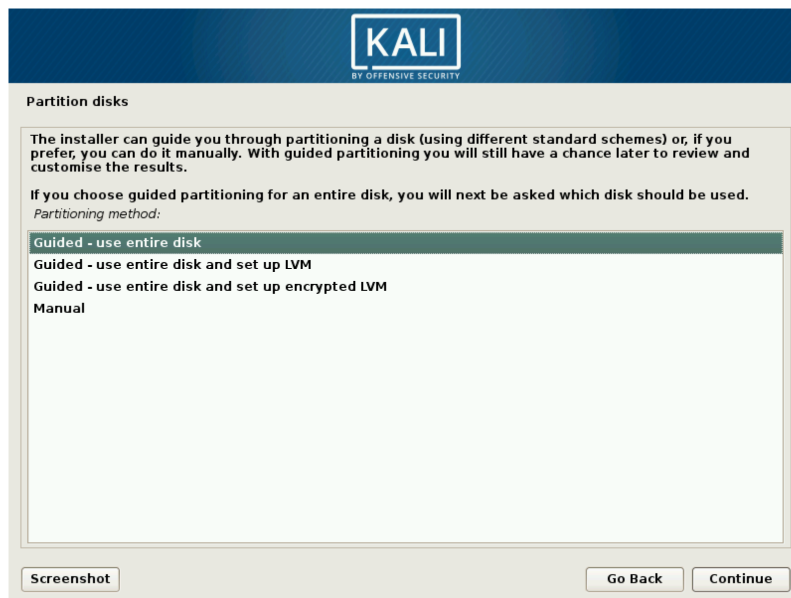
١.١٢.١.٢.٤ التقسيم الموجة

تعرض الشاشة الأولى في أداة التقسيم (الشكل ٨.٤ "اختيار وضع التقسيم") نقاط الدخول لأوضاع التقسيم الموجهة واليدوية. إن "إرشادات استخدام القرص بأكمله (Guided – use entire disk)" هو نظام التقسيم الأسهل والأكثر شيوعاً، والذي سيخصص قرصًا كاملًا لنظام Kali Linux.

يستخدم التحديدان التاليان (LVM) Logical Volume Manager لإعداد أقسام منطقية (بدلاً من المادية)، مشفرة اختيارياً. سنناقش LVM والتشفير لاحقًا في هذا الفصل.

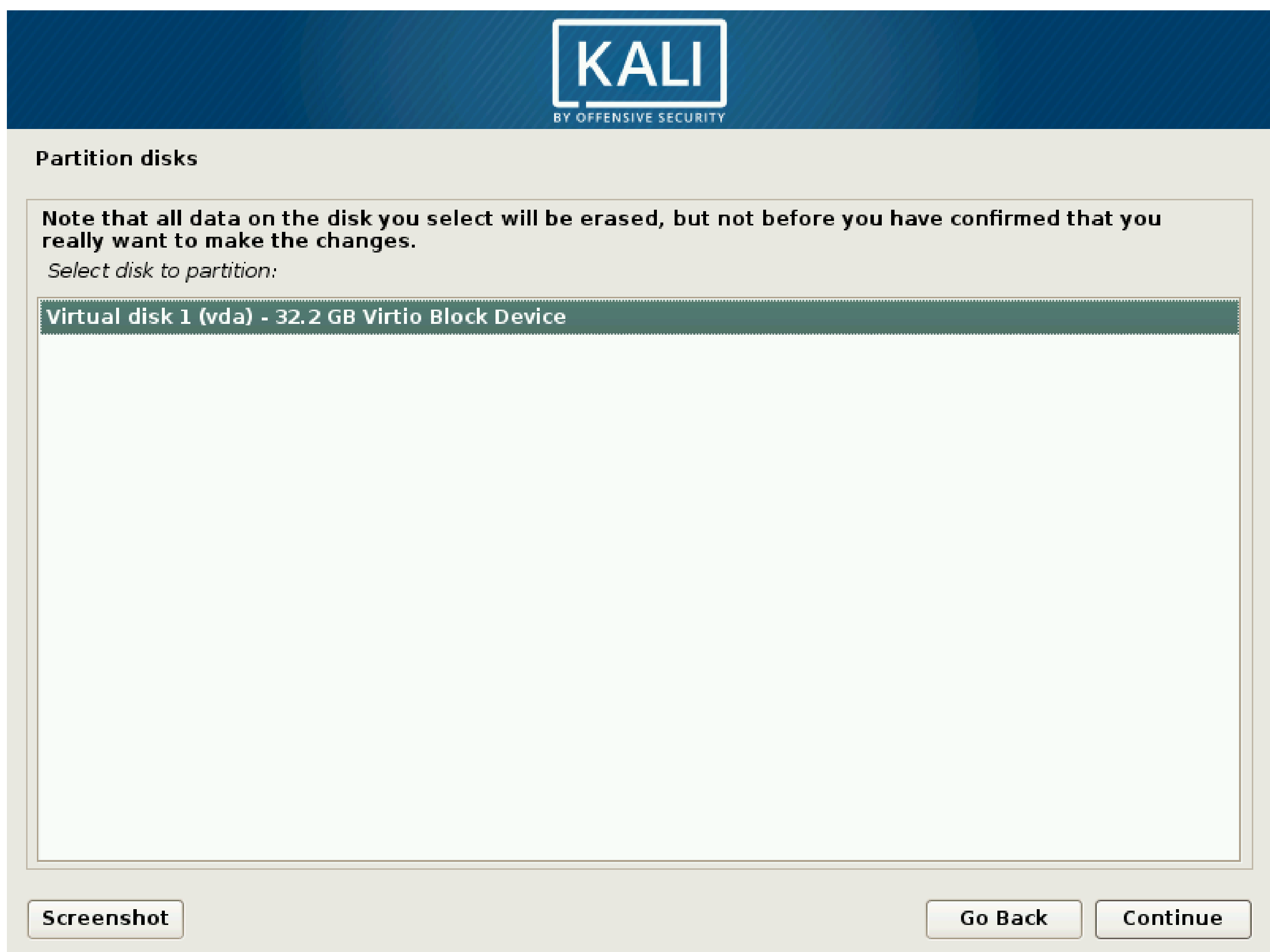
أخيرًا، يبدأ الخيار الأخير في التقسيم اليدوي، والذي يسمح بمزيد من مخططات التقسيم المتقدمة، مثل تثبيت Kali Linux إلى جانب أنظمة التشغيل الأخرى. سنناقش الوضع اليدوي في القسم التالي.

في هذا المثال، سنخصص قرصًا ثابتًا بالكامل لـ Kali، لذلك نختار " Guided – use entire disk " للمتابعة إلى الخطوة التالية.



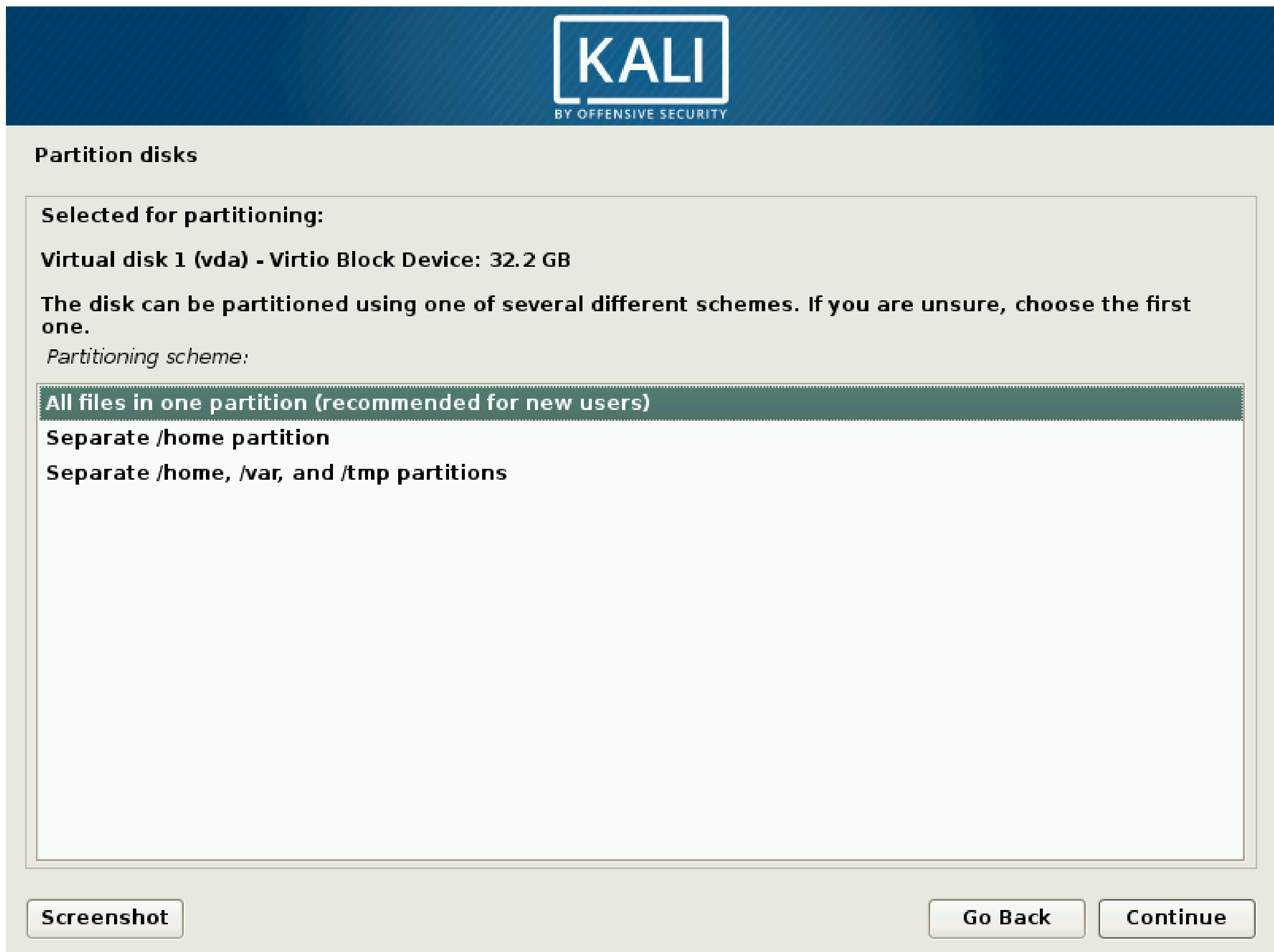
شكل ٨.٤. اختيار وضع التقسيم

تتيح لك الشاشة التالية (الموضحة في الشكل ٩.٤ "القرص المطلوب استخدامه للتقسيم الموجه") اختيار القرص الذي سيتم تثبيت Kali فيه عن طريق تحديد الإدخال المقابل (على سبيل المثال، "Virtual disk 1 (vda) – 32.2 GB Virtio Block Device"). بمجرد تحديده، سيستمر التقسيم الموجه. هذا الخيار سوف يمحو جميع البيانات الموجودة على هذا القرص، لذلك اختر بحكمة.



شكل ٩.٤. القرص المطلوب استخدامه للتقسيم الموجه

بعد ذلك، تقدم أداة التقسيم الموجهة ثلاث طرق تقسيم، والتي تتوافق مع استخدامات مختلفة، كما هو موضح في الشكل ٤.١٠، "تخصيص التقسيم الموجه".



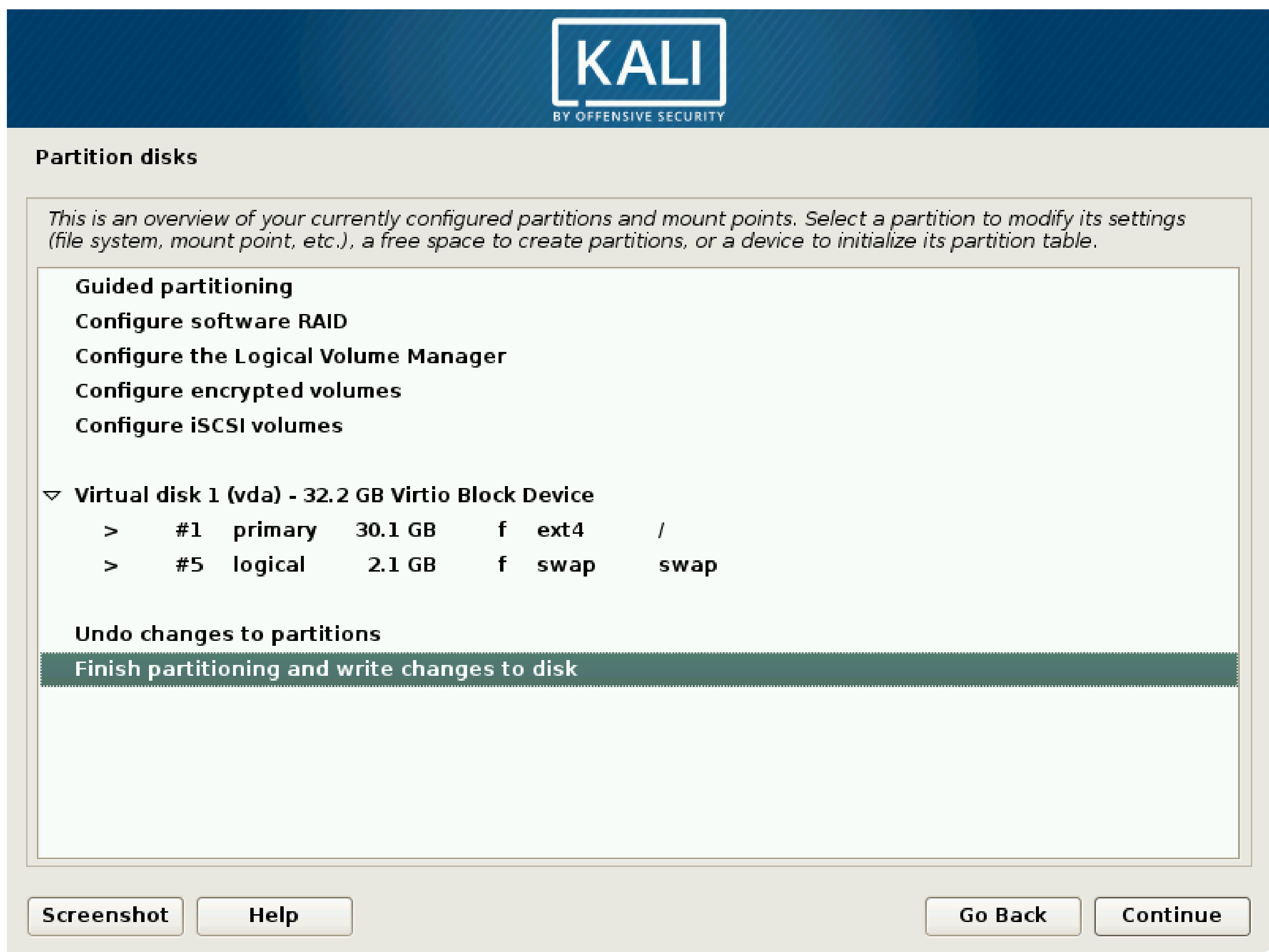
شكل ٤.١٠. تخصيص التقسيم الموجه

تسمى الطريقة الأولى "All files in one partition". يتم تخزين شجرة نظام Linux بالكامل في نظام ملفات واحد، يتوافق مع مجلد الجذر ("/"). يعمل نظام التقسيم البسيط والقوي هذا بشكل جيد على الأنظمة الشخصية أو أنظمة المستخدم الشخصية. على الرغم من الاسم، سيتم إنشاء قسمين بالفعل: الأول يضم النظام الكامل، والثاني الذاكرة الافتراضية (أو "المبادلة" "Swap").

تتشابه الطريقة الثانية، "Separate **/home/** partition"، ولكنها تقسم التسلسل الهرمي للملف إلى قسمين: قسم واحد يحتوي على نظام Linux (/)، والثاني يحتوي على "مجلدات home" (بمعنى بيانات المستخدم، في الملفات والمجلدات الفرعية متاح في **/home/**). من بين فوائد هذه الطريقة أنه من السهل الحفاظ على بيانات المستخدمين إذا كان عليك إعادة تثبيت النظام.

إن طريقة التقسيم الأخيرة، والتي تسمى "Separate **/home**, **/var**, and **/tmp** partitions"، مناسبة للخوادم وأنظمة المستخدمين المتعددين. يقسم شجرة الملفات إلى عدة أقسام: بالإضافة إلى أقسام الجذر **(/)** وحسابات المستخدمين (**/home/**)، كما أنه يحتوي على أقسام لبيانات برنامج الخادم (**/var/**)، والملفات المؤقتة (**/tmp/**). من فوائد هذه الطريقة أنه لا يمكن للمستخدمين قفل الخادم عن طريق استهلاك كل مساحة القرص الصلب المتاحة (يمكنهم فقط ملء **/tmp/** و **/home/**). في الوقت نفسه، لم تعد بيانات البرنامج الخفي (خاصة السجلات) تسد باقي النظام.

بعد اختيار نوع القسم، يقدم المثبت ملخصًا لاختياراتك على الشاشة كخريطة الأقسام (شكل ٤.١١. "التحقق من صحة التقسيم"). يمكنك تعديل كل قسم على حدة عن طريق تحديد قسم، على سبيل المثال: يمكنك اختيار نظام ملفات آخر إذا كان (*ext4*) غير مناسب. ومع ذلك، في معظم الحالات، يكون التقسيم المقترح معقولًا ويمكنك قبوله عن طريق اختيار " Finish partitioning and write changes to disk ". قد يستمر الأمر دون أن يقول ذلك، ولكن اختر بحكمة لأن هذا سيمحو محتويات القرص المحدد.



شكل ٤.١١. التحقق من صحة التقسيم

٢.١٢.١.٢.٤. التقسيم اليدوي

يتيح اختيار Manual في الشاشة الرئيسية "Partition disks" (شكل ٨.٤. "اختيار وضع التقسيم") مرونة أكبر، مما يسمح لك باختيار تكوينات أكثر تقدماً وإملاء غرض وحجم كل قسم على وجه التحديد. على سبيل المثال، يسمح لك هذا الوضع بتثبيت Kali إلى جانب أنظمة التشغيل الأخرى، وتمكين مجموعة متكررة قائمة على البرامج من الأقراص المستقلة " Redundant Array of Independent Disks"(RAID) لحماية البيانات من فشل القرص الصلب، وتغيير حجم الأقسام الموجودة بأمان دون فقدان البيانات، من بين أشياء أخرى.

إذا كنت مستخدمًا أقل خبرة يعمل على نظام يحتوي على بيانات حالية، فيرجى توخي الحذر الشديد مع طريقة الإعداد هذه، لأنه من السهل جدًا ارتكاب أخطاء قد تؤدي إلى فقدان البيانات.

تقليص قسم الوندوز

لتثبيت Kali Linux جنباً إلى جنب مع نظام تشغيل موجود (Windows أو غيره)، ستحتاج إلى مساحة متوفرة على القرص الصلب غير المستخدمة للأقسام المخصصة لـ Kali. في معظم الحالات، يعني هذا تقليص قسم موجود وإعادة استخدام المساحة المحررة.

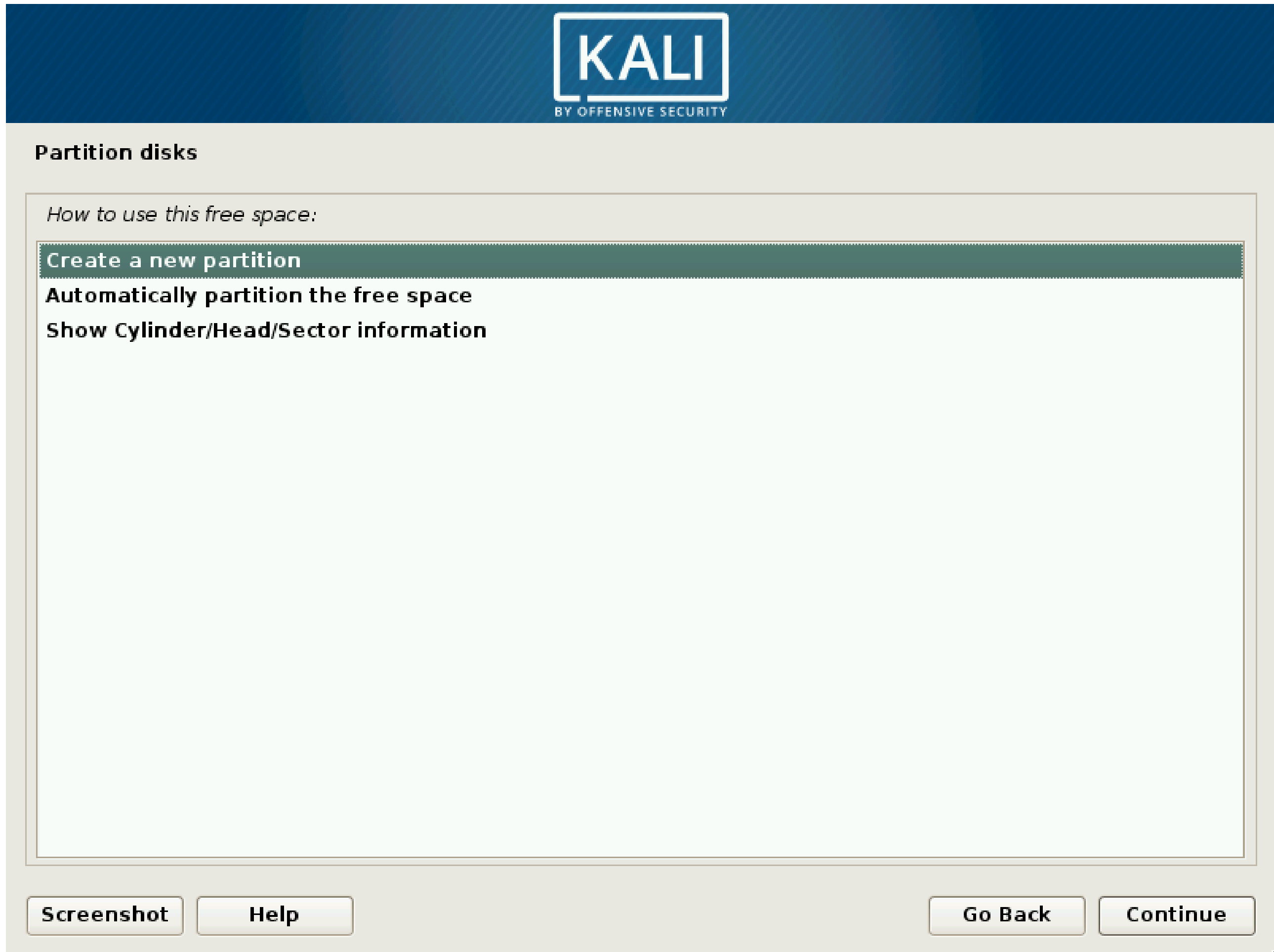
إذا كنت تستخدم وضع التقسيم اليدوي، فيمكن للمثبت تقليص قسم Windows بسهولة تامة. ما عليك سوى اختيار قسم Windows وإدخال حجمه الجديد (يعمل هذا مع كل من أقسام FAT وNTFS).

الشاشة الأولى في برنامج التثبيت اليدوي هي في الواقع نفس الشاشة الموضحة في الشكل ١١.٤. "التحقق من صحة التقسيم"، باستثناء أنه لا يتضمن أي أقسام جديدة لإنشائها. الأمر متروك لك لإضافة ذلك.

أولاً، سترى خيارًا لإدخال "Guided partitioning" متبوعًا بعدة خيارات تكوين. بعد ذلك، سيعرض برنامج التثبيت الأقراص المتوفرة وأقسامها وأي مساحة حرة ممكنة لم يتم تقسيمها بعد. يمكنك تحديد كل عنصر معروض والضغط على مفتاح **Enter** للتفاعل معه، كالمعتاد.

إذا كان القرص جديد تمامًا، فقد تضطر إلى إنشاء جدول أقسام. يمكنك القيام بذلك عن طريق اختيار القرص. بمجرد الانتهاء من ذلك، سترى مساحة حرة متوفرة داخل القرص.

للاستفادة من هذه المساحة الحرة، يجب عليك تحديدها وسيقدم لك المثبت طريقتين لإنشاء أقسام في تلك المساحة.



شكل ٤.١٢. إنشاء أقسام في المساحة الحرة

سيقوم الخيار الأول بإنشاء قسم واحد بالخصائص (بما في ذلك الحجم) من اختيارك. سيستخدم الإدخال الثاني كل المساحة الحرة وسيخلق أقساماً متعددة فيه بمساعدة معالج التقسيم الموجه (انظر القسم ٤.٢.١.١٢.١. "التقسيم الموجه"). يعد هذا الخيار ممتعاً بشكل خاص عندما تريد تثبيت Kali إلى جانب نظام تشغيل آخر ولكن عندما لا ترغب في إدارة تخطيط القسم بشكل دقيق. سيظهر الخيار الأخير أرقام cylinder/head/sector لبداية ونهاية المساحة الحرة.

عندما تختار "Create a new partition"، فسوف تدخل في سلسلة من تسلسل التقسيم اليدوي. بعد تحديد هذا الخيار، ستتم مطالبتك بحجم القسم. إذا كان القرص يستخدم جدول قسم MSDOS، فسيتم إعطاؤك خيار إنشاء قسم أساسي أو منطقي. (أشياء يجب معرفتها: لا يمكن أن

يكون لديك سوى أربعة أقسام أساسية ولكن هناك العديد من الأقسام المنطقية. القسم الذي يحتوي على /boot، تتبعه النواة، يجب أن يكون قسمًا أساسيًا، والأقسام المنطقية موجودة في قسم ممتد، يستهلك أحد الأقسام الأربعة الأساسية.) ثم سترى شاشة تكوين القسم العام:

KALI
BY OFFENSIVE SECURITY

Partition disks

You are editing partition #1 of Virtual disk 1 (vda). No existing file system was detected in this partition.
Partition settings:

Use as:	Ext4 journaling file system
Mount point:	/
Mount options:	defaults
Label:	none
Reserved blocks:	5%
Typical usage:	standard
Bootable flag:	off

Delete the partition
Done setting up the partition

Screenshot | Help | Go Back | Continue

شكل ٤.١٣. شاشة تكوين الأقسام

لتلخيص هذه الخطوة من التقسيم اليدوي، دعونا نلقي نظرة على ما يمكنك القيام به مع القسم الجديد. تستطيع:

❖ تنسيقه وتضمينه في شجرة الملفات عن طريق اختيار نقطة وصل.

نقطة الوصل: هو المجلد الذي سيضم محتويات نظام الملفات على القسم المحدد. وبالتالي، يُقصد عادةً بالقسم المُركب على **/home/** أن يحتوي على بيانات المستخدم، بينما يُعرف **"/"** باسم جذر شجرة الملفات، وبالتالي فإن قسم الجذر هو الذي سيستضيف نظام Kali بالفعل.

❖ استخدامه كقسم المبادلة. عندما تفتقر نواة Linux إلى ذاكرة حرة كافية، فإنها تخزن أجزاء غير نشطة من ذاكرة الوصول العشوائي في قسم المبادلة الخاص على القرص الثابت. يجعل النظام الفرعي للذاكرة الافتراضية هذا شفافًا للتطبيقات. لمحاكاة الذاكرة الإضافية، يستخدم Windows ملف المبادلة (الترحيل) الموجود مباشرة في نظام الملفات. على العكس من ذلك، يستخدم Linux قسمًا مخصصًا لهذا الغرض، ومن هنا يأتي مصطلح قسم التبادل.

❖ جَعْلَهُ "physical volume for encryption" لحماية سرية البيانات على أقسام معينة. تتم أتمتة هذه الحالة في التقسيم الموجه. انظر القسم ٢.٢.٤."التثبيت على نظام ملفات مشفرة بالكامل" لمزيد من المعلومات.

❖ جعله "حجمًا فعليًا لـ LVM" (غير مشمول في هذا الكتاب). لاحظ أن هذه الميزة يتم استخدامها بواسطة التقسيم الموجه عند إعداد أقسام مشفرة.

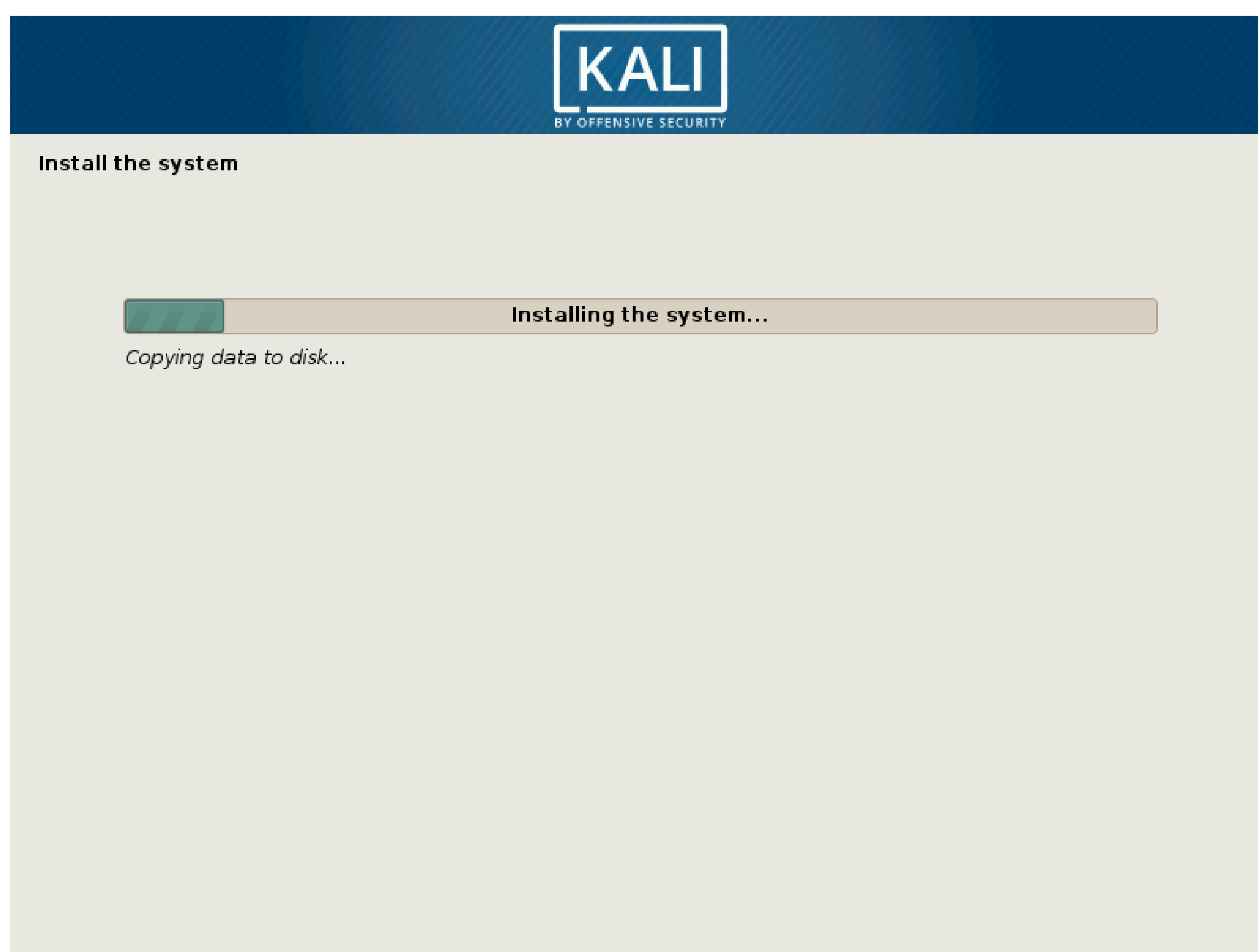
❖ استخدمه كجهاز RAID (غير مشمول في هذا الكتاب).

❖ اختيار عدم استخدام القسم واتركه دون تغيير.

عند الانتهاء، يمكنك إما الرجوع عن التقسيم اليدوي عن طريق اختيار "تراجع عن التغييرات إلى أقسام" أو كتابة التغييرات على القرص عن طريق تحديد "إنهاء التقسيم وكتابة التغييرات على القرص" من شاشة المثبت اليدوي (الشكل ١١.٤. "التحقق من صحة التقسيم").

١٣.١.٢.٤. نسخ الصورة المباشرة

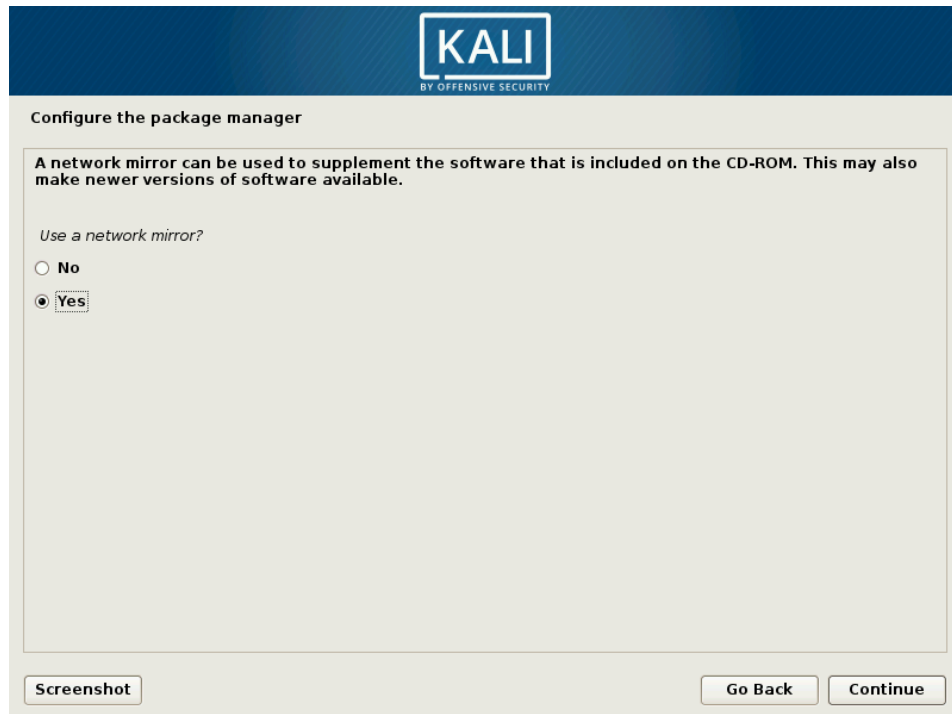
هذه الخطوة التالية، التي لا تتطلب أي تدخل من المستخدم، تنسخ محتويات الصورة المباشرة إلى نظام الملفات الهدف، كما هو موضح في الشكل ١٤.٤. "نسخ البيانات من الصورة المباشرة".



شكل ١٤.٤. نسخ البيانات من الصورة المباشرة

١٤.١.٢.٤. تكوين مدير الحزم (apt)

لكي تكون قادرًا على تثبيت برامج إضافية، يلزم تكوين APT وإخباره عن مكان حزم دبيان. في كالي، هذه الخطوة غير تفاعلية في أغلب الأحيان حيث نجبر المرآة على أن تكون **http.kali.org**. عليك فقط تأكيد ما إذا كنت تريد استخدام هذه النسخة المتطابقة (الشكل ١٥.٤. "استخدام مرآة شبكة؟"). إذا لم تستخدمها، فلن تتمكن من تثبيت حزم إضافية بـ **apt** إلا إذا قمت بتكوين مستودع الحزم لاحقًا.



شكل ١٥.٤. استخدام مرآة الشبكة؟

إذا كنت تريد استخدام نسخة متطابقة محلية بدلاً من **http.kali.org**، يمكنك تمرير اسمها في سطر أوامر النواة (في وقت الإقلاع) باستخدام بناء جملة مثل هذا:

```
mirror/http/hostname=my.own.mirror
```

أخيرًا، يقترح البرنامج استخدام وكيل *"proxy" HTTP* كما هو موضح في الشكل ١٦.٤. "استخدام وكيل HTTP". وكيل HTTP هو خادم يقوم بإعادة توجيه طلبات HTTP لمستخدمي الشبكة. يساعد في بعض الأحيان على تسريع التنزيلات عن طريق الاحتفاظ بنسخة من الملفات التي تم نقلها من خلالها (ثم نتحدث عن وكيل للتخزين المؤقت). في بعض الحالات، هي الوسيلة الوحيدة للوصول إلى خادم ويب خارجي؛ في مثل هذه الحالات، لن يتمكن المثبت من تنزيل حزم دبيان إلا إذا قمت بملء هذا الحقل بشكل صحيح أثناء التثبيت. إذا لم تقدم عنوانًا وكيلًا، فسيحاول المثبت الاتصال بالإنترنت مباشرةً.

شكل ١٦.٤. استخدام وكيل http

بعد ذلك، سيتم تنزيل ملفي **Packages.xz** و**Sources.xz** تلقائيًا لتحديث قائمة الحزم المعترف بها من قِبل APT.

١٥.١.٢.٤. تثبيت محمل الإقلاع GRUB

محمل الإقلاع هو أول برنامج يتم تشغيله بواسطة BIOS. يقوم هذا البرنامج بتحميل نواة Linux في الذاكرة ثم تنفيذها. يقدم محمل الإقلاع غالبًا قائمة تتيح لك اختيار النواة المراد تحميلها أو نظام التشغيل للإقلاع.

نظراً لتفوقها التقني، فإن GRUB هو مُحمّل الإقلاع الافتراضي الذي تم تثبيته بواسطة Debian: إنه يعمل مع معظم أنظمة الملفات، وبالتالي لا يحتاج إلى تحديث بعد كل تثبيت نواة جديدة؛ لأنه يقرأ التكوين أثناء الإقلاع ويعثر على الموضع الدقيق من النواة الجديدة.

يجب تثبيت GRUB على سجل الإقلاع الرئيسي (MBR) ما لم يكن لديك بالفعل نظام لينكس آخر مثبت يعرف كيفية تشغيل Kali Linux. كما هو موضح في الشكل ١٧.٤. "تثبيت محمل الإقلاع GRUB على القرص الصلب" ، إن تعديل MBR سيجعل أنظمة التشغيل غير المعترف بها والتي تعتمد عليها غير قابلة للإقلاع حتى تقوم بإصلاح تكوين GRUB.



شكل ١٧.٤. تثبيت محمل الإقلاع GRUB على القرص الصلب

في هذه الخطوة (الشكل ١٨.٤. "الجهاز المطلوب لتثبيت محمل الإقلاع عليه")، يجب عليك تحديد الجهاز الذي سيتم تثبيت GRUB عليه. يجب أن يكون هذا هو محرك الإقلاع الحالي.



شكل ١٨.٤. الجهاز المطلوب لتثبيت محمل الإقلاع عليه

احترس: محمل الإقلاع والإقلاع المزدوج

تكتشف هذه المرحلة من عملية التثبيت أنظمة التشغيل المثبتة بالفعل على الحاسوب وستقوم تلقائيًا بإضافة الإدخالات المقابلة في قائمة الإقلاع. ومع ذلك، ليس كل برامج التثبيت تفعل هذا.

على وجه الخصوص، إذا قمت بتثبيت (أو إعادة تثبيت) Windows بعد ذلك، سيتم محو أداة محمل الإقلاع. سيظل نظام Kali موجود على محرك الأقراص الثابت؛ ولكن لن يكون من الممكن الوصول إليه من قائمة الإقلاع. سيكون عليك حينئذٍ بدء برنامج تثبيت Kali باستخدام المعلمة:

```
rescue/enable=true
```

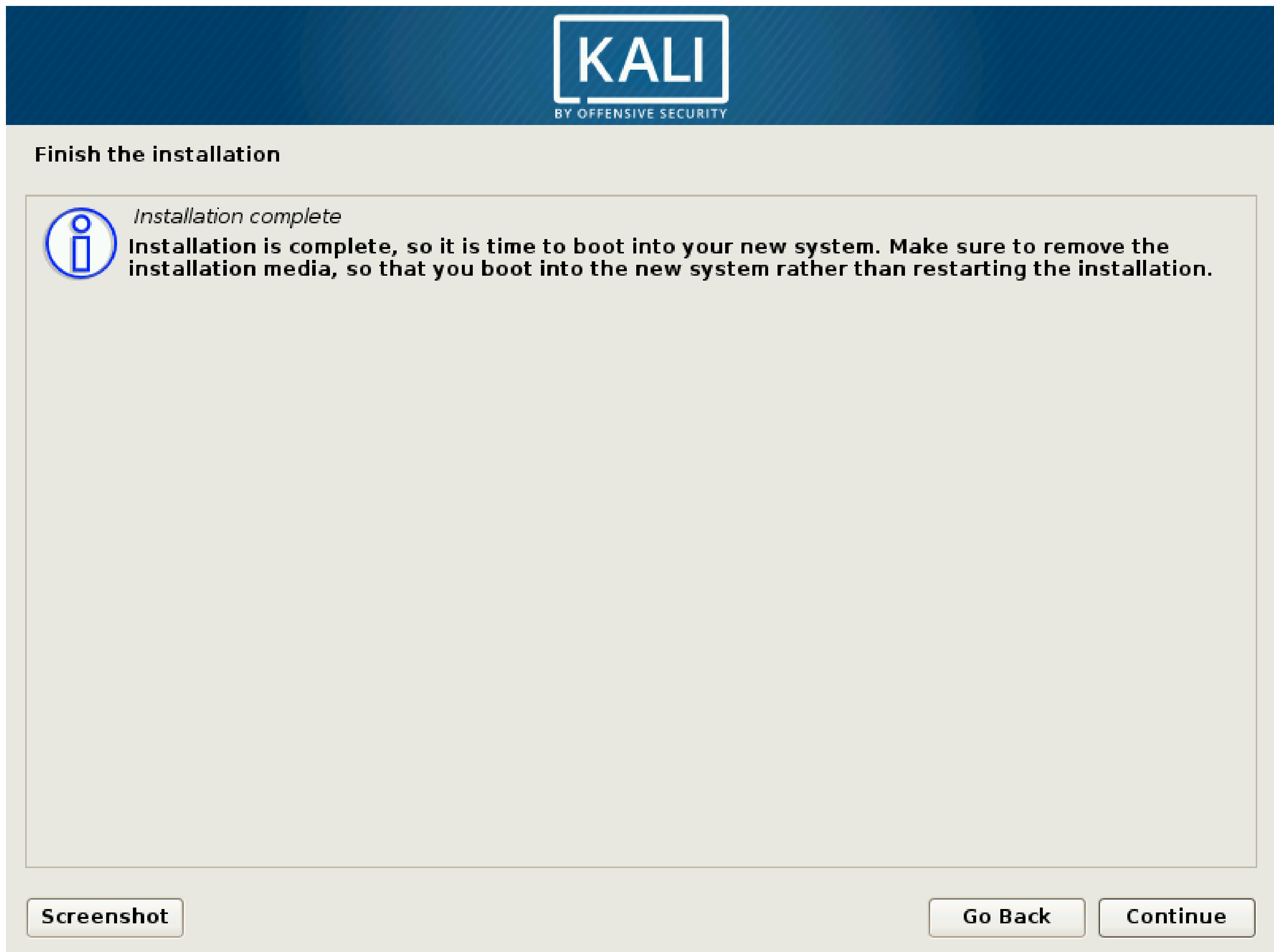
في سطر أوامر النواة لإعادة تثبيت أداة محمل الإقلاع. تم وصف هذه العملية بالتفصيل في دليل تثبيت ديبان.

http://www.debian.org/releases/stable/amd64/ch08s07.html

١٦.١.٢.٤. الانتهاء من التثبيت وإعادة التشغيل

الآن وبعد اكتمال التثبيت، يطلب منك البرنامج إزالة قرص DVD-ROM من القارئ (أو فصل محرك USB الخاص بك) حتى يتمكن جهاز الحاسوب من الإقلاع بنظام Kali الجديد الخاص بك بعد إعادة تشغيل برنامج التثبيت (الشكل ١٩.٤. "اكتمل التثبيت").

أخيرًا، سيقوم المثبت ببعض أعمال التنظيف، مثل إزالة الحزم الخاصة بإنشاء البيئة المباشرة.



شكل ١٩.٤. اكتمل التثبيت

٤.٢.٢. التثبيت بنظام ملفات مشفر بالكامل

لضمان سرية بياناتك، يمكنك إعداد أقسام مشفرة. سيؤدي ذلك إلى حماية بياناتك في حالة فقد الحاسوب المحمول أو القرص الصلب أو سرقته. يمكن لأداة التقسيم مساعدتك في هذه العملية، سواء في الوضع الإرشادي أو اليدوي.

سيجمع وضع التقسيم الموجه بين استخدام تقنيتين:

لتشفير الأقسام **L**inux **U**nified **K**ey **S**etup (LUKS)

لإدارة التخزين بشكل حيوي **L**ogical **V**olume **M**anagement (LVM)

يمكن أيضًا ضبط كلتا الميزتين وتكوينهما من خلال وضع التقسيم اليدوي.

٤.٢.٢.١. مقدمة في LVM

دعونا نناقش LVM أولاً. باستخدام مصطلحات LVM، القسم الافتراضي هو وحدة تخزين منطقية، والتي تعد جزءًا من مجموعة وحدات تخزين أو مجموعة من عدة وحدات تخزين فعلية. وحدات التخزين الفعلية هي أقسام حقيقية (أو أقسام افتراضية يتم تصديرها بواسطة أدوات تجريدية أخرى، مثل جهاز RAID للبرنامج أو قسم مشفر).

بفضل الافتقار إلى التمييز بين الأقسام "المادية" و "المنطقية"، يتيح لك LVM إنشاء أقسام "افتراضية" تمتد على عدة أقراص. الفوائد ذات شقين: لم يعد حجم الأقسام محددًا من قِبل الأقراص الفردية ولكن بواسطة حجمها التراكمي، ويمكنك تغيير حجم الأقسام الموجودة في أي وقت، مثل بعد إضافة قرص إضافي.

تعمل هذه التقنية بطريقة بسيطة للغاية: يتم تقسيم كل وحدة تخزين، سواء كانت مادية أو منطقية، إلى كتل من نفس الحجم، والتي يرتبط بها LVM. تؤدي إضافة قرص جديد إلى إنشاء وحدة

تخزين فعلية جديدة توفر كتَلًا جديدة يمكن ربطها بأي مجموعة وحدات تخزين. يمكن لجميع الأقسام الموجودة في مجموعة مستوى الصوت الاستفادة الكاملة من المساحة المخصصة الإضافية.

٢.٢.٢.٤. مقدمة إلى LUKS

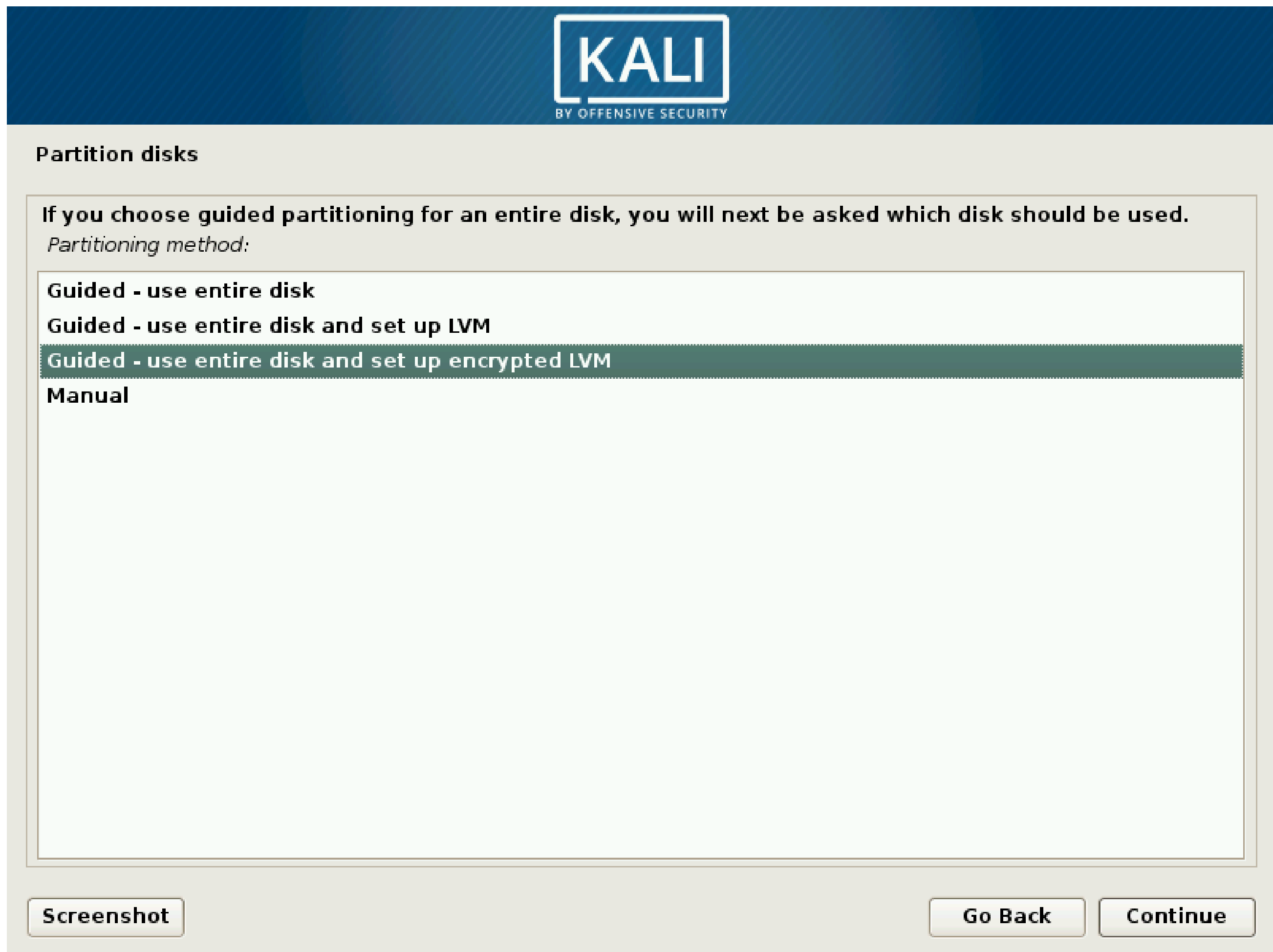
لحماية بياناتك، يمكنك إضافة طبقة تشفير أسفل نظام الملفات الذي تختاره. يستخدم Linux (وخاصة برنامج تشغيل *dm-crypt*) معين الجهاز لإنشاء القسم الافتراضي (الذي تكون محتوياته محمية) استنادًا إلى قسم أساسي يقوم بتخزين البيانات في نموذج مشفر (بفضل LUKS). يقيس LUKS تخزين البيانات المشفرة وكذلك معلومات التعريف التي تشير إلى خوارزميات التشفير المستخدمة.

تشفير قسم المبادلة

عند استخدام قسم مشفر، يتم تخزين مفتاح التشفير في الذاكرة (RAM)، وعند الإسبات، يقوم الحاسوب المحمول بنسخ المفتاح، إلى جانب محتويات أخرى من ذاكرة الوصول العشوائي، إلى قسم المبادلة للقرص الثابت. نظرًا لأن أي شخص لديه حق الوصول إلى ملف المبادلة (بما في ذلك فني أو لص) يمكنه استخراج المفتاح وفك تشفير بياناتك، فيجب حماية ملف المبادلة بالتشفير.
ولهذا السبب، سوف يحذرك برنامج التثبيت إذا حاولت استخدام قسم مشفر إلى جانب قسم تبديل غير مشفر. في سطر أوامر النواة لإعادة تثبيت أداة محمل الإقلاع. تم وصف هذه العملية بالتفصيل في دليل تثبيت ديبان.
http://www.debian.org/releases/stable/amd64/ch08s07.html

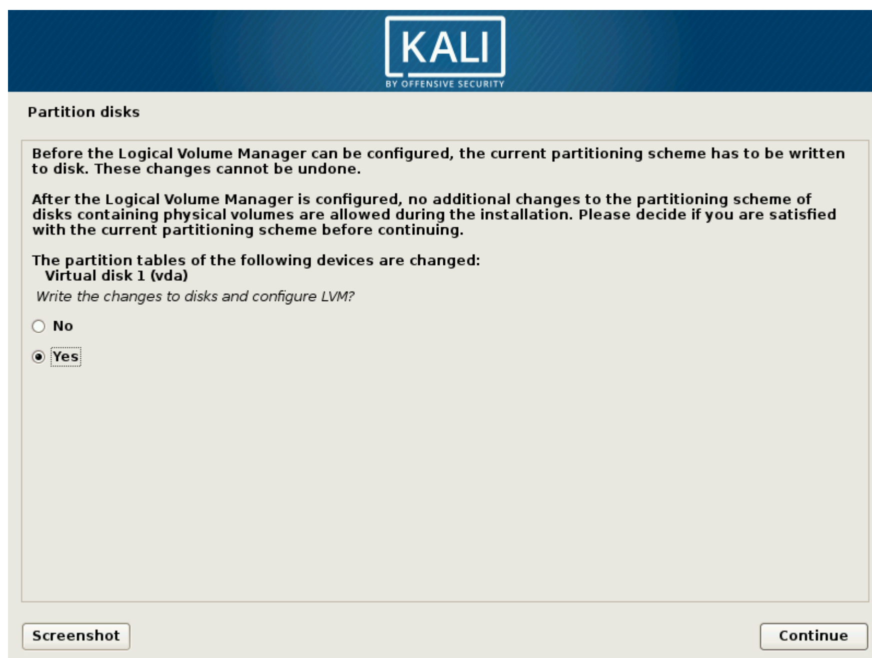
٣.٢.٢.٤. إعداد أقسام مشفرة

إن عملية تثبيت LVM المشفرة هي نفس عملية التثبيت القياسية باستثناء خطوة التقسيم (الشكل ٤.٢٠. "Guided Partitioning with Encrypted LVM") حيث ستختار بدلاً من ذلك "Guided – use entire disk and set up encrypted LVM". ستكون النتيجة نظامًا لا يمكن إقلاعه أو الوصول إليه حتى يتم توفير كلمة مرور التشفير. سيؤدي ذلك إلى تشفير وحماية البيانات الموجودة على القرص.



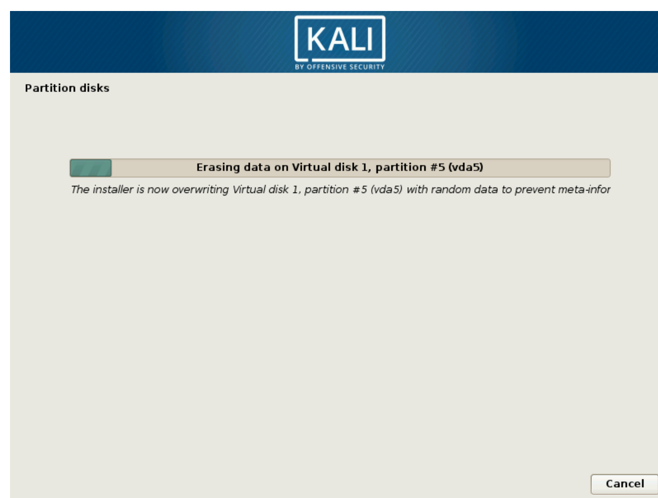
شكل ٤.٢٠. Guided Partitioning with Encrypted LVM

سيقوم مُثبّت التقسيم الموجه تلقائيًا بتعيين قسم فعلي لتخزين البيانات المشفرة، كما هو موضح في الشكل ٢١.٤. "تأكيد التغييرات على جدول الأقسام". في هذه المرحلة، سيقوم المثبت بتأكيد التغييرات قبل كتابتها على القرص.



شكل ٢١.٤. تأكيد التغييرات على جدول الأقسام

ثم يتم تهيئة هذا القسم الجديد ببيانات عشوائية، كما هو موضح في الشكل ٢٢.٤. "محو البيانات على القسم المشفر". هذا يجعل المناطق التي تحتوي على بيانات لا يمكن تمييزها عن المناطق غير المستخدمة، مما يجعل من الصعب اكتشاف البيانات المشفرة، ومن ثم مهاجمتها.



الشكل ٢٢.٤. محو البيانات على القسم المشفر

بعد ذلك، يطلب منك برنامج التثبيت إدخال كلمة مرور فك التشفير (الشكل ٢٣.٤."أدخل كلمة مرور فك التشفير"). لعرض محتويات القسم المشفر، ستحتاج إلى إدخال كلمة المرور هذه في كل مرة تقوم فيها بإعادة تشغيل النظام. لاحظ التحذير الموجود في برنامج التثبيت: سيكون نظامك المشفر قويًا بقدر قوة كلمة المرور هذه.

KALI
BY OFFENSIVE SECURITY

Partition disks

You need to choose a passphrase to encrypt Virtual disk 1, partition #5 (vda5).

The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.

A good passphrase will contain a mixture of letters, numbers and punctuation. Passphrases are recommended to have a length of 20 or more characters.

Encryption passphrase:

Show Password in Clear

Please enter the same passphrase again to verify that you have typed it correctly.

Re-enter passphrase to verify:

Show Password in Clear

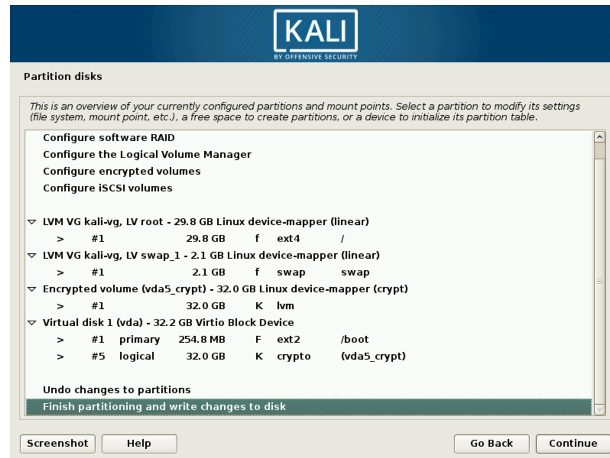
Screenshot | Go Back | Continue

شكل ٢٣.٤. ادخل كلمة مرور فك التشفير

تمتع أداة التقسيم الآن بالوصول إلى قسم افتراضي جديد يتم تخزين محتوياته مشفرة في القسم الفعلي الأساسي. نظرًا لأن LVM يستخدم هذا القسم الجديد كوحدة تخزين فعلية، يمكنه حماية عدة أقسام (أو وحدات تخزين منطقية LVM) باستخدام مفتاح التشفير نفسه، بما في ذلك قسم المبادلة (انظر الشريط الجانبي Encrypted Swap Partition). هنا، لا يتم استخدام LVM لتسهيل توسيع حجم التخزين، ولكن فقط من أجل توفير الراحة غير المباشرة التي تسمح بتقسيم قسم مشفر واحد إلى وحدات تخزين منطقية متعددة.

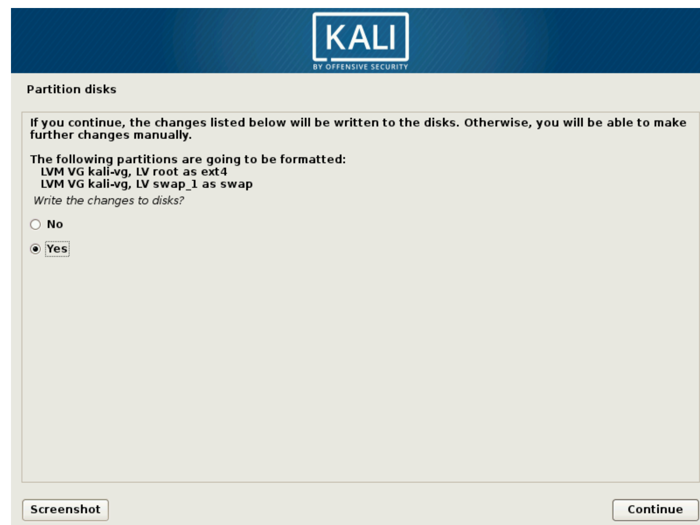
٤.٢.٢.٤. نهاية التقسيم الموجه باستخدام LVM المشفر

بعد ذلك، يتم عرض مخطط التقسيم الناتج (الشكل ٢٤.٤. "التحقق من صحة التقسيم لتثبيت LVM المشفر") حتى تمكن من تعديل الإعدادات حسب الحاجة.



شكل ٢٤.٤. التحقق من صحة التقسيم لتثبيت LVM المشفر

أخيرًا، بعد التحقق من صحة إعداد القسم، تطلب الأداة تأكيد كتابة التغييرات على الأقراص، كما هو موضح في الشكل ٢٥.٤. "تأكيد الأقسام المراد تنسيقها".



شكل ٢٥.٤. تأكيد الأقسام المراد تنسيقها

أخيرًا، تستمر عملية التثبيت كالمعتاد كما هو موضح في القسم ١٤.١.٢.٤. "تكوين مدير الحزم (**apt**)".

٣.٤. التثبيت الغير مراقب

يعد مثبّتا دبيان وكالي نمطيًا للغاية: على المستوى الأساسي، ينفّذان فقط العديد من البرامج النصية (مجموعة في حزم صغيرة تسمى udeb — لـ µdeb أو micro-deb) واحدة تلو الأخرى. يعتمد كل برنامج نصي على debconf (راجع أداة **debconf**)، التي تتفاعل معك والمستخدم وتخزين معلمات التثبيت. لهذا السبب، يمكن أيضًا تثبيت برنامج التثبيت تلقائيًا من خلال أتمتة debconf preseeding، وهي دالة تتيح لك تقديم إجابات غير مراقبة لأسئلة التثبيت.

١.٣.٤. الإجابات المعدة مسبقا

هناك طرق متعددة لاستباق الإجابات على المثبت. كل أسلوب له مزاياه وعيوبه. بناءً على وقت حدوث عملية التغذية السابقة، تختلف الأسئلة التي يمكن إجراؤها.

١.١.٣.٤. بمعلمات الإقلاع

يمكنك أن تسبق أي سؤال مثبّت مع معلمات الإقلاع تنتهي في سطر أوامر النواة، يمكن الوصول إليها من خلال proc/cmdline/. ستتيح لك بعض أدوات تحميل الإقلاع تحرير هذه المعلمات بشكل تفاعلي (وهو أمر عملي لأغراض الاختبار)، ولكن إذا كنت تريد إجراء التغييرات، فسيتعين عليك تعديل تكوين أداة تحميل الإقلاع.

يمكنك استخدام المعرف الكامل لأسئلة debconf مباشرةً (مثل debian-installer/language=en) أو يمكنك استخدام الاختصارات للأسئلة الأكثر

شيوعًا (مثل `language=en` أو `hostname=duke`). انظر القائمة الكاملة للأسماء المستعارة -aliases- في دليل تثبيت دبيان.

لا يوجد أي قيود على الأسئلة التي يمكنك إجراؤها لأن معلمات الإقلاع متوفرة من بداية عملية التثبيت وتتم معالجتها في وقت مبكر جدًا. ومع ذلك، يقتصر عدد معلمات الإقلاع على 32 وعددًا من تلك المعلمات يتم استخدامها بالفعل افتراضيًا. من المهم أيضًا إدراك أن تغيير تكوين محمل الإقلاع يمكن أن يكون غير تافه في بعض الأحيان.

في القسم ٣.٩، "Building Custom Kali Live ISO Images"، ستتعلم أيضًا كيفية تعديل تكوين Isolinux عند إنشاء صورة Kali ISO الخاصة بك.

٢.١.٣.٤. بملف preseed في البداية

يمكنك إضافة ملف باسم preseed.cfg في جذر initrd الخاص بالمثبت (هذا هو initrd الذي يُستخدم لبدء المثبت). عادةً ما يتطلب ذلك إعادة إنشاء حزمة مصدر debian-installer لإنشاء إصدارات جديدة من initrd. ومع ذلك، يوفر التصميم المباشر طريقة مناسبة للقيام بذلك، وهو موضح بالتفصيل في القسم ٣.٩، "صور مخصصة بناء Kali Live ISO".

لا تحتوي هذه الطريقة أيضًا على أية قيود على الأسئلة التي يمكنك إجراؤها نظرًا لأن ملف preseed متاح فور بدء التشغيل. في كالي، استفدنا بالفعل من هذه الميزة لتخصيص سلوك مثبت دبيان الرسمي.

٣.١.٣.٤. مع ملف Preseed في Boot Media

يمكنك إضافة ملف مسبق على وسائط الإقلاع (CD أو مفتاح USB)؛ يحدث ذلك قبل بدء الوسائط، مما يعني مباشرة بعد الأسئلة حول تخطيط اللغة ولوحة المفاتيح. يمكن استخدام معلمة الإقلاع preseed/file للإشارة إلى موقع ملف preseed (على سبيل المثال، cdrom/preseed.cfg/ عند التثبيت من قرص مضغوط أو hd-media/preseed.cfg/ عند التثبيت من مفتاح USB).

لا يجوز لك تقديم إجابات على خيارات اللغة والبلد حيث يتم تحميل ملف preseeding لاحقًا في العملية، بمجرد تحميل برامج تشغيل الأجهزة. على الجانب الإيجابي، تجعل عملية الإنشاء المباشر من السهل وضع ملف إضافي في صور ISO التي تم إنشاؤها (انظر القسم ٣.٩، "صور مخصصة بناء Kali Live ISO").

٤.١.٣.٤. بملف preseed محمل من الشبكة

يمكنك إتاحة ملف مسبق على الشبكة من خلال خادم ويب وإخبار المثبت بتنزيل هذا الملف قبل إضافة معلمة الإقلاع:

preseed/url=http: //server/preseed.cfg أو باستخدام عنوان) url "المستعار alias.")

ومع ذلك، عند استخدام هذه الطريقة، تذكر أنه يجب تكوين الشبكة أولاً. هذا يعني أن أسئلة debconf المتعلقة بالشبكة (خاصة اسم المضيف واسم المجال) وجميع الأسئلة السابقة (مثل اللغة والبلد) لا يمكن إعطاؤها بهذه الطريقة. غالبًا ما يتم استخدام هذه الطريقة مع معلمات الإقلاع التي تسبق هذه الأسئلة المحددة.

طريقة التجميع هذه هي الأكثر مرونة حيث يمكنك تغيير تكوين التثبيت دون تغيير وسائط التثبيت.

تأخير أسئلة اللغة، البلد، لوحة المفاتيح

للتغلب على قيود عدم القدرة على الافتراض على أسئلة اللغة والدولة ولوحة المفاتيح، يمكنك إضافة معلمة الإقلاع `auto-install/enable=true` (أو `auto = true`). باستخدام هذا الخيار، سيتم طرح الأسئلة لاحقًا في هذه العملية، بعد تهيئة الشبكة، وبالتالي بعد تنزيل الملف الرئيسي.
الجانب السلبي هو أن الخطوات الأولى (لا سيما تكوين الشبكة) ستحدث دائمًا باللغة الإنجليزية، وإذا كانت هناك أخطاء، فسيتعين على المستخدم العمل من خلال شاشات باللغة الإنجليزية (مع تكوين لوحة مفاتيح في(QWERTY).

4.3.2. إنشاء ملفpreseed

ملف preseed هو ملف نصي عادي يحتوي فيه كل سطر على إجابة سؤال Debconf واحد. يتم تقسيم السطر لأربعة حقول مفصولة بمسافة بيضاء (مسافات أو tabs). على سبيل المثال،

```
d-i mirror/suite string kali-rolling:
```

- ❖ يشير الحقل الأول إلى صاحب السؤال. على سبيل المثال، يتم استخدام "d-i" للأسئلة المتعلقة بالمثبت (installer) || لعله اختصار لـ "debian installer"||. قد ترى أيضًا اسم حزمة للأسئلة الواردة من حزم دبيان (كما في هذا المثال: atftpd atftpd / use_inetd boolean false).
- ❖ الحقل الثاني هو معرف للسؤال.
- ❖ يسرد الحقل الثالث نوع السؤال.
- ❖ يحتوي الحقل الرابع والأخير على قيمة الإجابة المتوقعة. لاحظ أنه يجب فصله عن الحقل الثالث بمسافة واحدة؛ تعتبر أحرف المسافات الإضافية جزءًا من القيمة.

إن أبسط طريقة لكتابة ملف preseed هي تثبيت النظام يدويًا. ثم سيقدم الأمر:

```
debconf-get-selections - installer
```

الإجابات التي قدمتها للمثبت. يمكنك الحصول على إجابات موجهة إلى الحزم الأخرى باستخدام:

```
debconf-get-selections
```

ومع ذلك، فإن الحل الأنظف هو كتابة الملف يدويًا، بدءًا من المثال ثم المرور بالوثائق. باستخدام هذا النهج، يمكن فقط توقع الأسئلة التي تحتاج إلى تجاوز الإجابة الافتراضية. قدّم معلمة الإقلاع:

```
priority=critical
```

لـ (مرشد ديبيان) Instruct Debconf إلى طرح الأسئلة المهمة فقط، واستخدام الإجابة الافتراضية للباقي.

ملحق دليل التثبيت

يحتوي دليل تثبيت دبيان، المتاح عبر الإنترنت، على وثائق تفصيلية حول استخدام ملف preseed في الملحق. كما يشمل أيضا ملف مفصل وتعليقات بسيطة، يمكن أن يكون بمثابة قاعدة للتخصيصات المحلية.

https://www.debian.org/releases/stable/amd64/apb.html

https://www.debian.org/releases/stable/example-preseed.txt

لاحظ أن الروابط السابقة توثق الإصدار المستقر من دبيان وأن كالي يستخدم الإصدار (Debian testing)، لذا فقد تواجه اختلافات بسيطة. يمكنك أيضًا الرجوع إلى دليل التثبيت المستضاف على موقع مشروع مثبت ديبيان (Debian-installer). قد يكون أكثر حداثة.

٤.٤. تثبيت على أجهزة ARM

يعمل Kali Linux على مجموعة متنوعة من الأجهزة المستندة إلى ARM (أجهزة الحاسوب المحمولة وأجهزة الحاسوب المضمنة ولوحات المطورين، على سبيل المثال) ولكن لا يمكنك استخدام مثبت Kali التقليدي على هذه الأجهزة نظراً لأنها غالبًا ما تكون لها متطلبات محددة فيما يتعلق بتكوين النواة أو محمل الإقلاع.

لجعل هذه الأجهزة في متناول مستخدمي Kali، قامت Offensive Security بتطوير نصوص برمجية لإنشاء صور قرص جاهزة للاستخدام لأجهزة ARM المختلفة. توفر هذه الصور للتنزيل على موقعها على الويب:

https://www.offensive-security.com/kali-linux-arm-images/

نظراً لأن هذه الصور متاحة، فإن مهمتك في تثبيت Kali على جهاز ARM بسيطة لحد كبير. وهنا الخطوات الأساسية:

- ❖ قم بتنزيل الصورة لجهاز ARM الخاص بك وتأكد من أن المجموع الاختباري يطابق الموجود على موقع الويب (انظر القسم ٣.١.٢، "التحقق من النزاهة والأصالة" للحصول على توضيحات حول كيفية القيام بذلك). لاحظ أن الصور عادةً ما تكون مضغوطة بتنسيق xz، تأكد من إلغاء ضغطها باستخدام **unxz**.
- ❖ اعتماداً على فتحة توسيع التخزين المتاحة على أجهزة ARM الخاص بك، احصل على بطاقة SD أو بطاقة SD صغيرة أو وحدة eMMC بسعة 8 GB على الأقل.
- ❖ انسخ الصورة التي تم تنزيلها إلى جهاز التخزين باستخدام **dd**. هذا مشابه لعملية نسخ صورة ISO على مفتاح USB (انظر القسم ٤.١.٢. "نسخ الصورة على قرص DVD-ROM أو مفتاح USB").

```
dd if=kali-image.img of=/dev/something bs=512k
```

- ❖ قم بتوصيل بطاقة SD/eMMC بجهاز ARM الخاص بك.

❖ قم بتشغيل جهاز ARM وقم بتسجيل الدخول إليه (المستخدم "root"، كلمة المرور "toor") ||هذا قديما، أما الأن kali/kali||. إذا لم يكن لديك شاشة متصلة، فسيتعين عليك معرفة عنوان IP الذي تم تعيينه عبر DHCP والاتصال بهذا العنوان عبر SSH. تحتوي بعض خوادم DHCP على أدوات أو واجهات ويب لإظهار leases الحالية. إذا لم يكن لديك أي شيء من هذا القبيل، فاستخدم الشم (sniffer) للبحث عن حركة مرور DHCP lease.

❖ قم بتغيير كلمة المرور وقم بإنشاء مفاتيح مضيف SSH جديدة، خاصة إذا كان الجهاز سيتم تشغيله بشكل دائم على شبكة عامة! الخطوات بسيطة نسبيًا، راجع إنشاء مفاتيح مضيف SSH جديدة.

❖ استمتع بجهاز ARM الجديد الذي يعمل بنظام Kali Linux!

حالات خاصة ووثائق أكثر تفصيلاً

هذه الإرشادات عامة، وبينما تعمل مع معظم الأجهزة، هناك دائمًا استثناءات. على سبيل المثال، تتطلب أجهزة Chromebook وضع المطور وتتطلب الأجهزة الأخرى ضغطًا خاصًا على المفاتيح للإقلاع من الوسائط الخارجية.

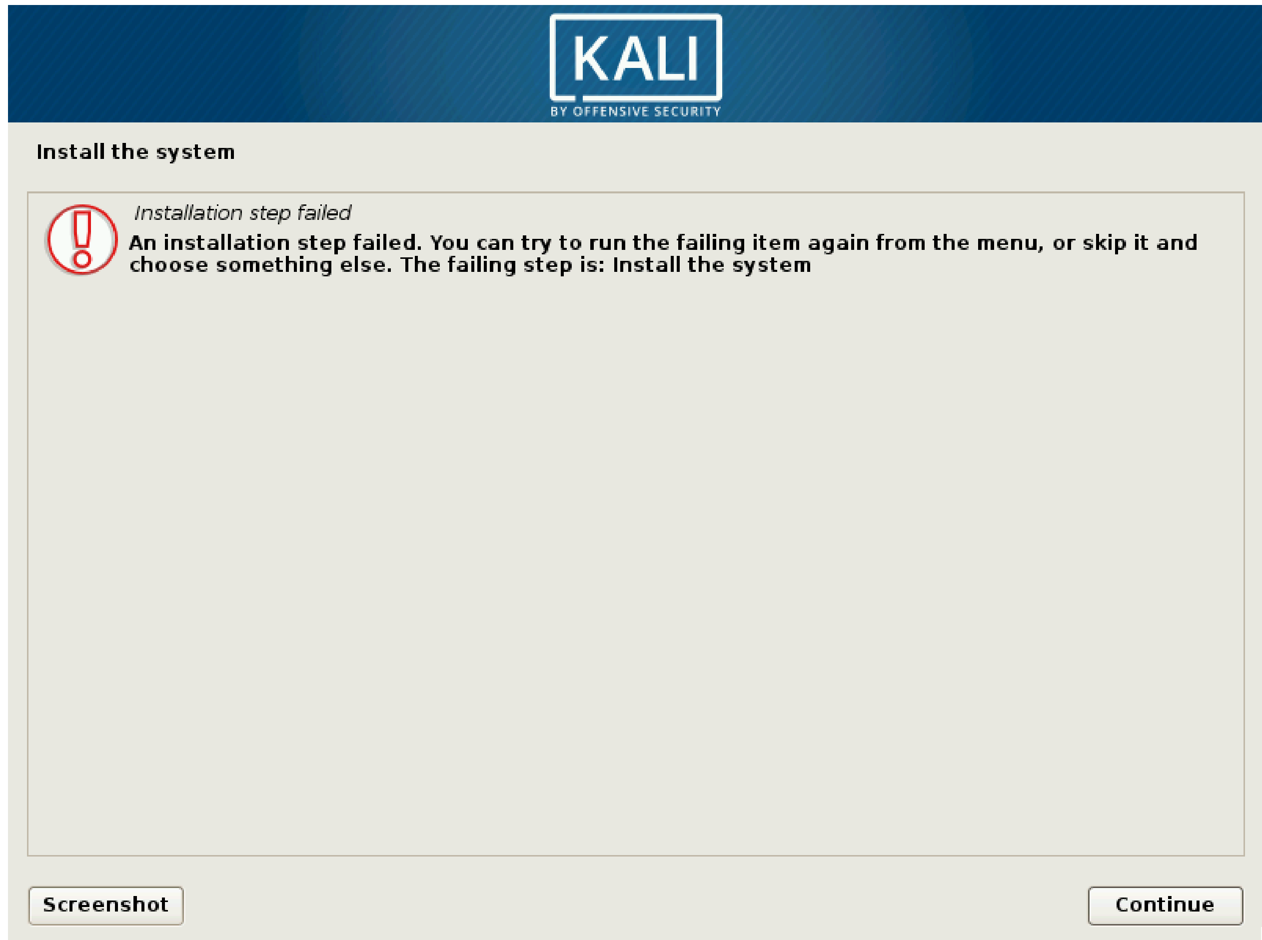
نظرًا لأن أجهزة ARM تُضاف بشكل متكرر نسبيًا ومواصفاتها حيوية للغاية، فلن نغطي تعليمات التثبيت المحددة لأجهزة ARM المختلفة هنا. بدلاً من ذلك، ارجع إلى قسم "Kali on ARM" المخصص في موقع وثائق Kali للحصول على معلومات حول كل أجهزة ARM المدعوم بواسطة Offensive Security:

http://docs.kali.org/category/kali-on-arm

٥.٤ استكشاف أخطاء التثبيت وإصلاحها

المثبت موثوق للغاية، ولكن قد تواجه أخطاء أو تواجه مشاكل خارجية مثل: مشاكل الشبكة، والمرايا السيئة، ومساحة القرص غير كافية. وبسبب هذا، من المفيد جدًا أن تكون قادرًا على استكشاف المشكلات التي تظهر في عملية التثبيت وإصلاحها.

عندما يفشل برنامج التثبيت، سيظهر لك شاشة غير مفيدة إلى حد ما مثل الشاشة الموضحة في الشكل ٢٦.٤ "فشل خطوة التثبيت".



شكل ٢٦.٤ "فشل خطوة التثبيت"

في هذه المرحلة، من الجيد أن تعرف أن المثبت يستخدم وحدات تحكم افتراضية متعددة: الشاشة الرئيسية التي تراها تعمل إما على وحدة التحكم الخامسة (للمثبت الرسومي، **CTRL + Alt + F5**) أو على وحدة التحكم الأولى (للمثبت النصي، **Shift + F4**). في كلتا الحالتين، تعرض وحدة التحكم الرابعة (**CTRL + Shift + F4**) سجلات لما يحدث ويمكنك عادةً رؤية رسالة خطأ أكثر فائدة هناك، مثل تلك الموجودة في الشكل ٢٧.٤. "شاشة السجل للمثبت"، والتي يكشف أن مساحة المثبت قد نفدت.

```
tion:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 88:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/choose_partition/60partition_tree/do_op
tion:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 88:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/free_space/50new/do_option:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 226:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/free_space/50new/do_option:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 226:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: DEBUG: resolver (libgcc1): package doesn't exist (ignored)
Apr 15 19:04:24 main-menu[833]: INFO: Menu item 'live-installer' selected
Apr 15 19:04:24 base-installer: info: Using squashfs support for /cdrom/live/filesystem.squashfs
Apr 15 19:04:24 anna-install: Installing squashfs-modules
Apr 15 19:04:24 anna[8545]: DEBUG: resolver (kernel-image-4.3.0-kali1-amd64-di): package doesn't exi
st (ignored)
Apr 15 19:04:24 anna[8545]: DEBUG: retrieving squashfs-modules-4.3.0-kali1-amd64-di 4.3.3-5kali4
Apr 15 19:04:24 kernel: [  165.758382] squashfs: version 4.0 (2009/01/31) Phillip Lougher
Apr 15 19:04:24 kernel: [  165.764051] loop: module loaded
Apr 15 19:04:45 base-installer: error: The tar process copying the live system failed (only 9238 out
 of 119223 files have been copied, last file was ).
Apr 15 19:04:45 main-menu[833]: (process:8491): tar: write error: No space left on device
Apr 15 19:04:45 main-menu[833]: (process:8491): tar: write error: Broken pipe
Apr 15 19:04:45 main-menu[833]: WARNING **: Configuring 'live-installer' failed with error code 1
Apr 15 19:04:45 main-menu[833]: WARNING **: Menu item 'live-installer' failed.
_
```

شكل ٢٧.٤. "شاشة السجل للمثبت"

الكونسول الثاني والثالث (**CTRL + Shift + F2** و **CTRL + Shift + F3**، على التوالي) صدفات المضيف التي يمكنك استخدامها للتحقيق في الوضع الحالي بمزيد من التفاصيل. يتم توفير معظم أدوات سطر الأوامر بواسطة BusyBox لذا فإن مجموعة الميزات محدودة نوعًا ما، ولكنها كافية لمعرفة معظم المشاكل التي من المحتمل أن تواجهها.

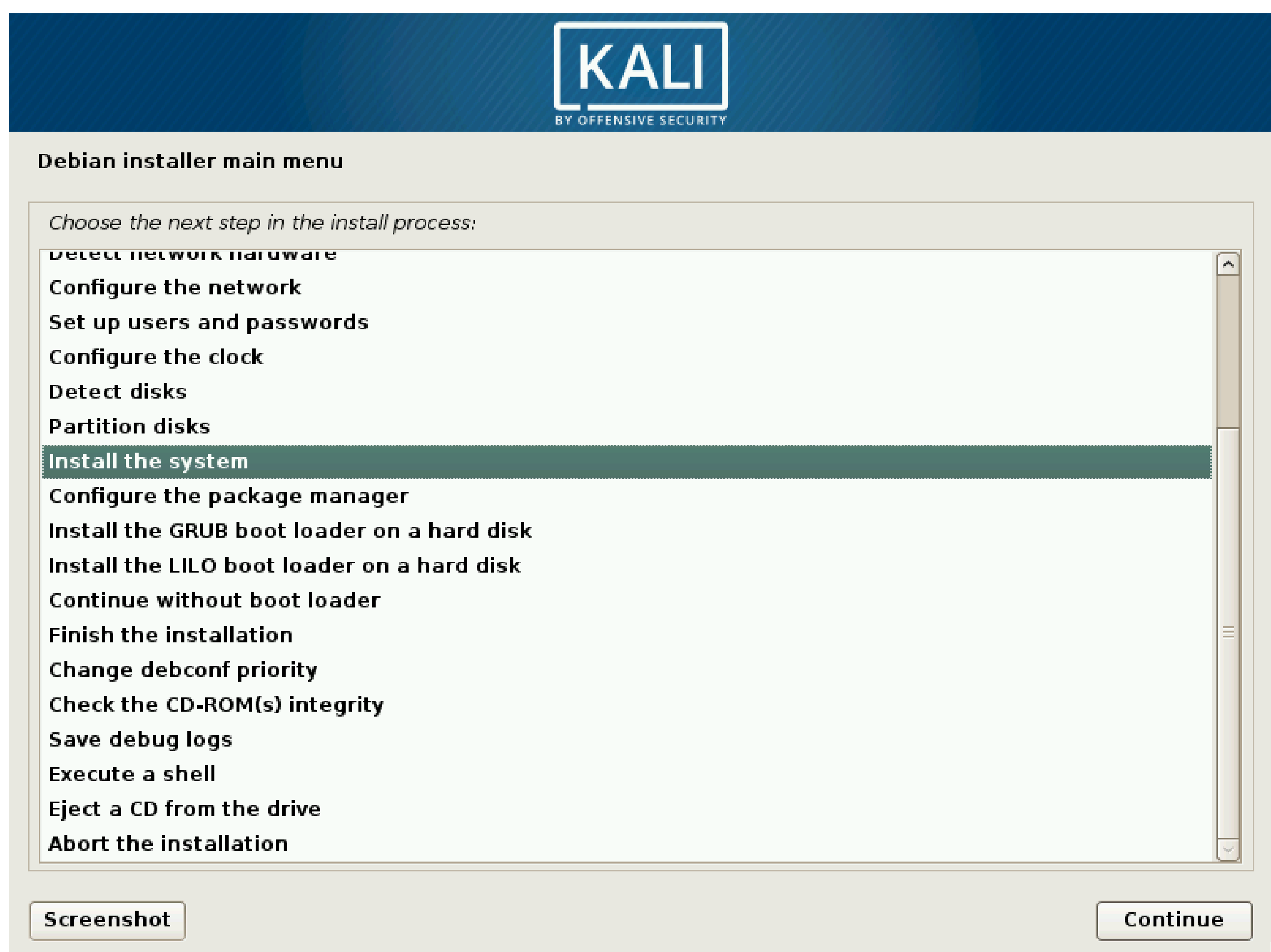
ما يمكن القيام به في صدفة المثبت

يمكنك فحص قاعدة بيانات debconf وتعديلها باستخدام `debconf-get` و `debconf-set`. تعتبر هذه الأوامر ملائمة بشكل خاص لاختبار قيم الـ preseeding.

يمكنك فحص أي ملف (مثل سجل التثبيت الكامل المتوفر في **/var/log/syslog**) بأمر **`cat`** أو **`more`**. يمكنك تعديل أي ملف باستخدام الأمر **`nano`**، بما في ذلك جميع الملفات المثبتة على النظام. سيتم وصل نظام الملفات الجذر بـ **target/** بمجرد اكتمال خطوة التقسيم لعملية التثبيت.

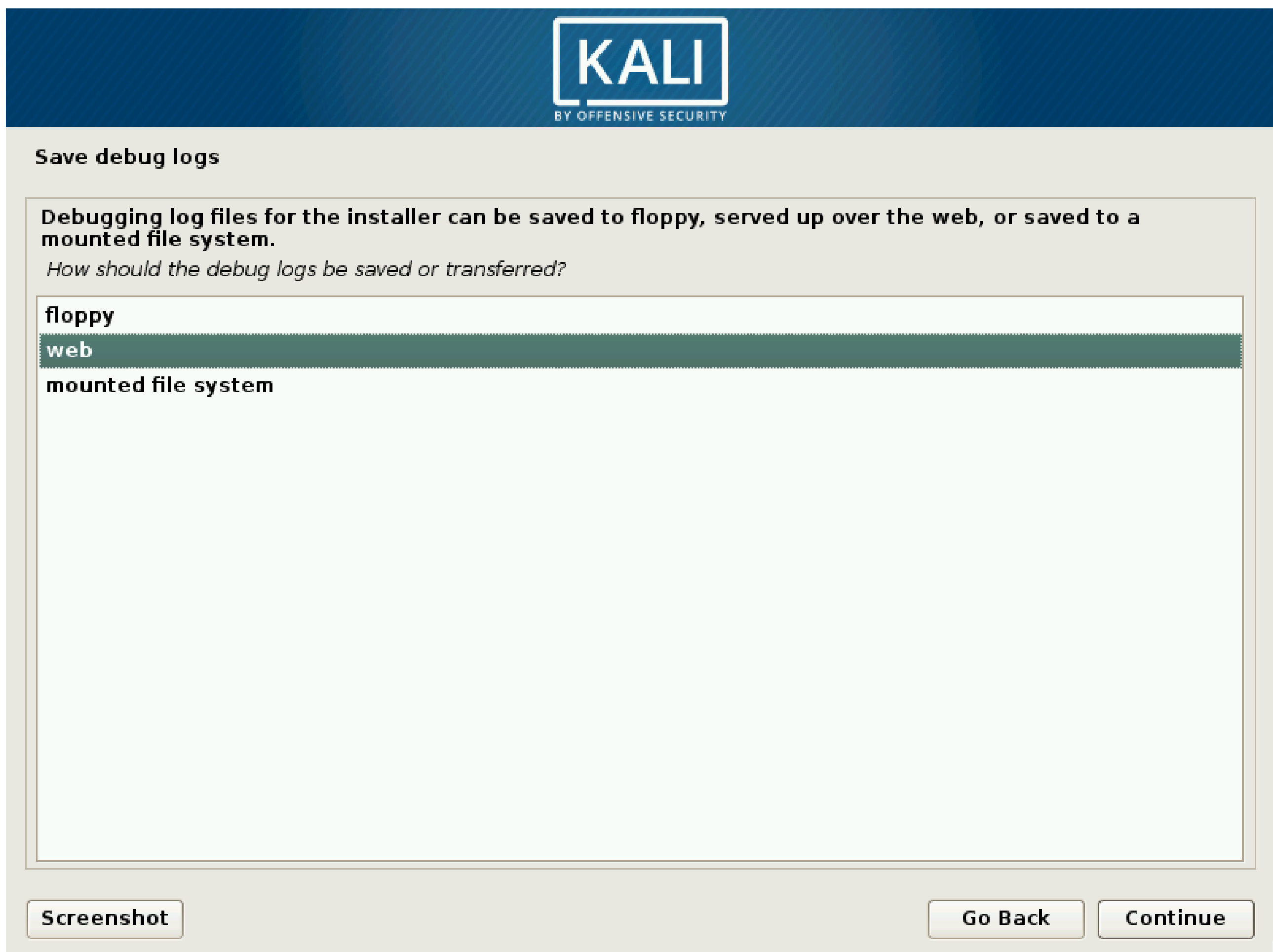
بمجرد تكوين الوصول إلى الشبكة، يمكنك استخدام **`wget`** و (netcat) **`nc`** لاسترداد البيانات وتصديرها عبر الشبكة.

بمجرد النقر فوق "**متابعة**" من شاشة فشل التثبيت الرئيسية (الشكل ٢٦.٤ "فشل خطوة التثبيت")، ستتم إعادتك إلى شاشة لن تراها عادةً (القائمة الرئيسية الموضحة في الشكل ٢٨.٤ "القائمة الرئيسية للمثبت")، مما يسمح لك بتشغيل خطوات التثبيت واحدة تلو الأخرى. إذا تمكنت من إصلاح المشكلة من خلال الوصول إلى الصدفة shell (تهانينا!)، فيمكنك إعادة محاولة الخطوة التي فشلت.



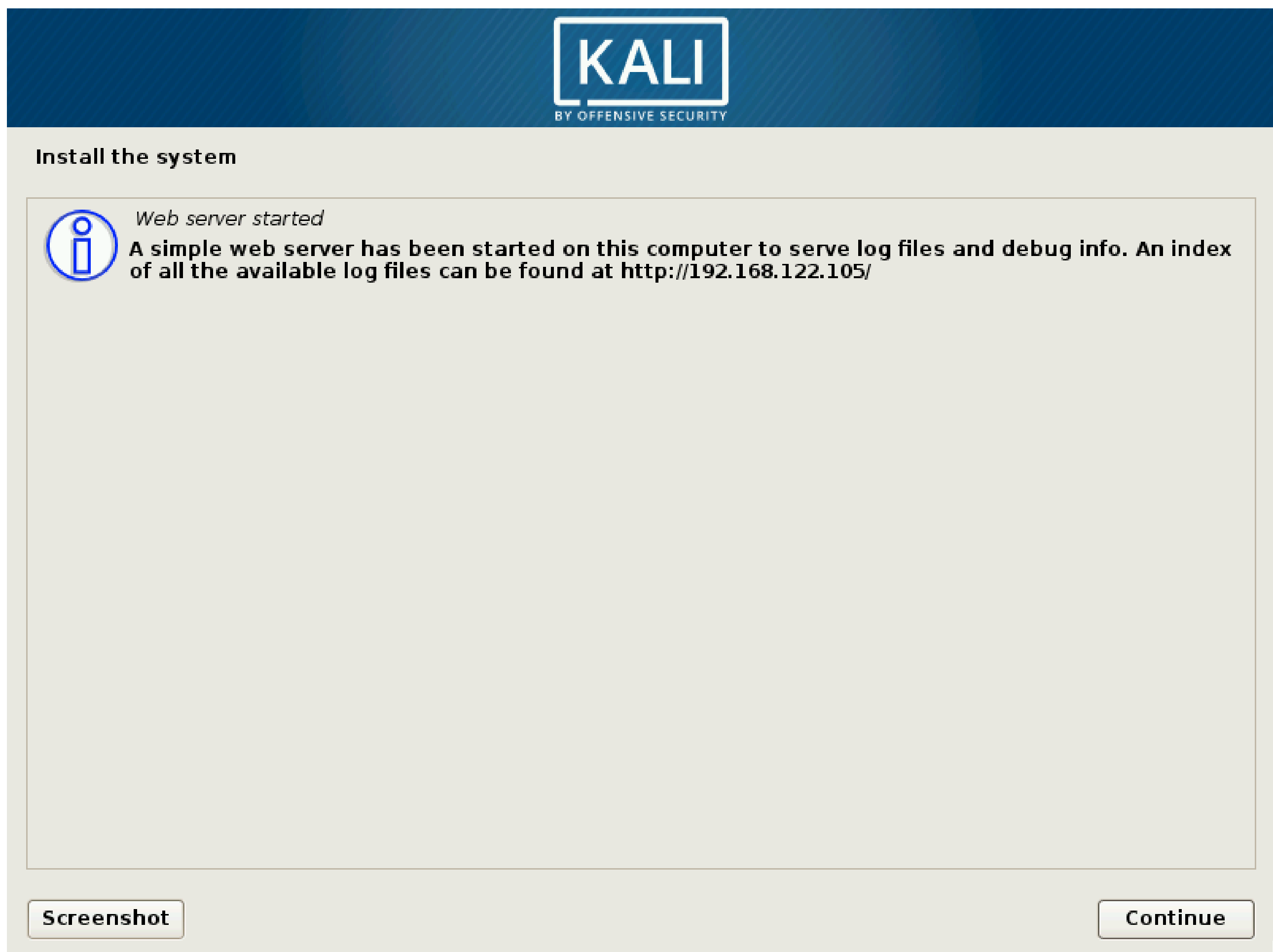
شكل ٢٨.٤ "القائمة الرئيسية للمثبت"

إذا كنت غير قادر على حل المشكلة، فقد تحتاج إلى تقديم تقرير خطأ. يجب أن يتضمن التقرير بعد ذلك سجلات المثبت، والتي يمكنك استردادها باستخدام وظيفة "حفظ سجلات تصحيح الأخطاء" "Save debug logs" في القائمة الرئيسية. يوفر طرقًا متعددة لتصدير السجلات، كما هو موضح في الشكل ٢٩.٤ "حفظ سجلات التصحيح (٢/١)".



شكل ٢٩.٤ "حفظ سجلات التصحيح (٢/١)

الطريقة الأكثر ملاءمة، والطريقة التي نوصي بها، هي السماح للمثبت ببدء خادم ويب يستضيف ملفات السجل (الشكل ٣٠.٤ "حفظ سجلات التصحيح (٢/٢)"). يمكنك بعد ذلك تشغيل متصفح من حاسوب آخر على نفس الشبكة وتنزيل جميع ملفات السجل ولقطات الشاشة التي التقطتها باستخدام زر **لقطة الشاشة "ScreenShot"** المتاح في كل شاشة.



شكل ٣٠.٤ "حفظ سجلات التصحيح (٢/٢) "

٦.٤. ملخص

في هذا الفصل، ركزنا على عملية تثبيت Kali Linux. ناقشنا الحد الأدنى من متطلبات التثبيت لـ Kali Linux، وعملية التثبيت لأنظمة الملفات القياسية والمشفرة بالكامل، والـ pre-seeding، والتي تسمح بالتثبيتات غير المراقبة "unattended"، وكيفية تثبيت Kali Linux على مختلف أجهزة ARM، وما الذي تفعله في حالات فشل التثبيت النادرة.

نصائح التلخيص:

❖ تختلف متطلبات التثبيت لـ Kali Linux من خادم SSH أساسي بدون سطح مكتب، مثل ذاكرة وصول عشوائي بسعة 128 MB (512 MB موصى بها) ومساحة قرص 2 GB، للـ:

higher-end kali-linux-full meta-package

❖ مع الحد الأدنى 2048 MB من ذاكرة الوصول العشوائي و 20 GB من مساحة القرص. بالإضافة إلى ذلك، يجب أن يحتوي جهازك على وحدة معالجة مركزية (CPU) مدعومة على الأقل ببنية amd64 أو i386 أو armel أو armhf أو arm64.

❖ يمكن تثبيت Kali بسهولة كنظام تشغيل أساسي، أو إلى جنب أنظمة تشغيل أخرى من خلال التقسيم وتعديل محمل الإقلاع، أو كنظام افتراضي.

❖ لضمان سرية بياناتك، يمكنك إعداد أقسام مشفرة. سيؤدي ذلك إلى حماية بياناتك في حالة فقدان أو سرقة الحاسوب المحمول أو محرك الأقراص الثابتة.

❖ يمكن أيضًا تشغيل المثبت تلقائيًا من خلال تصحيح debconf، وهي وظيفة تسمح لك بتقديم إجابات غير مراقبة على أسئلة التثبيت.

❖ ملف preseed هو ملف نصي عادي يحتوي على عدة أسطر كل سطر يكون إجابة سؤال Debconf واحد. يتم تقسيم السطر على أربعة حقول مفصولة بمسافة بيضاء (مسافات أو tabs). يمكنك الحصول على إجابات مسبقة للمثبت عن طريق معلمات الإقلاع، مع ملف preseed في البداية، أو ملف preseed على وسائط الإقلاع، أو مع ملف preseed من الشبكة.

❖ يعمل Kali Linux على مجموعة متنوعة من الأجهزة القائمة على ARM مثل أجهزة الحاسوب المحمولة وأجهزة الحاسوب المدمجة ولوحات المطور. تثبيت ARM واضح إلى حد ما. قم بتنزيل الصورة الصحيحة، وقم بنسخها على بطاقة SD، أو محرك أقراص USB، أو وحدة تحكم مدمجة للوسائط المتعددة (eMMC)، وقم بتوصيلها، وإقلاع جهاز ARM، والعثور على جهازك على الشبكة، وتسجيل الدخول، وتغيير كلمة مرور SSH ومفاتيح مضيف SSH.

❖ يمكنك تصحيح عمليات التثبيت الفاشلة باستخدام وحدات التحكم الافتراضية (يمكن الوصول إليها باستخدام CTRL + Shift ومفاتيح الوظائف)، وأوامر debconf-get و debconf-set، أو قراءة ملف سجل /var/log/syslog، أو عن طريق إرسال تقرير خطأ مع استرداد ملفات السجل بوظيفة "حفظ سجلات التصحيح" "Save debug logs" الخاصة بالمثبت.

الآن بعد أن ناقشنا أساسيات Linux وتثبيت Kali Linux، دعنا نناقش التكوين حتى تتمكن من البدء في تخصيص Kali لتناسب احتياجاتك.

التمرين الأول، للفصل الرابع - تثبيت مشفر القرص الكامل لـ Kali Linux

١. ما هو الحد الأدنى من الموارد المطلوبة لـ VM؟

٢. قم بتثبيت تشفير قياسي كامل افتراضي لـ Kali Linux على VM جديد. تأكد من أن الـ VM النهائي في وضع NAT.

٣. ما هي التقنيات المستخدمة للتشفير؟

الإجابات:

١. نأمل أنك لم تكن بحاجة إلى هذه الإجابة حقًا، وقد ألقيت نظرة خاطفة لأنك كنت فضوليًا. RAM 2 GB، 20 GB مساحة على القرص!

٢. تحقق من الفصل الرابع لإجراءات التثبيت. للتوضيح، الهدف هنا هو تثبيت Kali بنظام الملفات المشفر على VM جديد عن طريق الإقلاع من ISO والمتابعة يدويًا خلال التثبيت. الهدف ليس تشغيل ملف vmx. الموفر من Kali.

٣. LUKS وLogical Volume Management (LVM).

التمرين الثاني للفصل الرابع: التثبيت غير المراقب لـ Kali Linux

١. إنشاء VM جديد، بالحد الأدنى من المتطلبات.

٢. أكمل التثبيت القياسي، الافتراضي، باستخدام ملف preseed - مستضاف عبر HTTP (أو HTTPS). ملفك المضغوط هو:

https://www.kali.org/dojo/preseed.cfg .

٣. تأكد من أن التثبيت غير مراقب تمامًا: يجب عليك تحديد اللغة وخريطة لوحة المفاتيح واسم المضيف والمجال.

الإجابات:

١. الحد الأدنى من المتطلبات: GB 2 من ذاكرة الوصول العشوائي، مساحة القرص 20 GB. أنت تعرف هذا الآن، أليس كذلك؟

٢. هذا إلى حد كبير تثبيت قياسي عن طريق معلمات الإقلاع المعدلة. فيما يلي معلمات إقلاع مقترحة:

```
preseed/url=https://www.kali.org/dojo/preseed.cfg
locale=en_US keymap=us hostname=kali domain=local.
lan
```

لاحظ أن معلمات locale وkeymap وhostname وdomain توضع على سطر أوامر النواة!

```
                    GNU GRUB  version 2.02~beta3-5

setparams 'Start installer'

        linux        /install/gtk/vmlinuz video=vesa:ywrap,mtrr vga=788 preseed/url\
=https://www.kali.org/dojo/preseed.cfg locale=en_US keymap=us hostname=kalima domai\
n=local.lan_
        initrd        /install/gtk/initrd.gz
```

سؤال زن: "لماذا لا يمكن لـ preseed اليدوي أن يتعامل مع معلمات اللغة وخريطة المفاتيح واسم المضيف والمجال؟"

سؤال جيد. تعتمد معلمات Preseeding على الطريقة المتنبأ بها. إذا كنت تستخدم ملفًا تم تقديره في الحرف الأول، فيمكنك عندئذٍ توقع جميع المعلمات حتى تلك التي كانت في وقت مبكر جدًا من العملية. إذا كنت تستخدم ملفًا preseed من الشبكة أو من صورة ISO نفسها، فسيتم تطبيق المتوقع بعد ذلك بقليل في عملية التثبيت ويلزم توقع المعلمات المبكرة في سطر أوامر النواة.

وبدلاً من ذلك، يمكنك أيضًا استخدام المعلمات **auto=true** و`priority=critical`.

```
preseed/url=https://www.kali.org/dojo/preseed.cfg
auto=true priority=critical
```

إذا لم تكن تعرف هذا، صعد لعبتك! انتبه! تم ذكر معلمات الإقلاع التلقائي والأولويات بشكل خاص في الفصل ٤.٣. لا تعتقد أنه يمكنك تخطي كل المواد وتمريرها. نحن نراقبك.

التمرين الثالث، الفصل الرابع - تثبيت ARM القياسي لـ Kali Linux

إذا كان لديك Raspberry Pi أو جهاز مشابه، فاخذ نسخة من صورة ARM المناسبة من هنا (https://www.offensive-security.com/kali-linux-arm-images/). انسخه على بطاقة SD وجربه.

الإجابة:

هناك مشكلة الدجاج والبيض هنا. للحفاظ على توحيد الأمور، نفضل أن تقوم بتنفيذ كل هذه الخطوات في كالي. بهذه الطريقة، لديك كل الأدوات التي تحتاجها، ويمكننا إرشادك من خلالها دون شرح العملية على أنظمة تشغيل متعددة (Windows وOS X وLinux). ولكن من أجل القيام بذلك من كالي، نحتاج إلى نقل الصورة إلى كالي والطريقة الأكثر موثوقية ومباشرة للقيام بذلك هي بـ **scp** الذي يعتمد على خدمة **ssh**. لكننا لن نتطرق لـ SSH حتى الفصل التالي.

لذا، على الرغم من أنها ليست مثالية، إلا أننا سنغض الطرف عن إجراء SSH هنا حتى نتمكن من المضي قدمًا وسنناقش تفاصيل أكثر في الفصل التالي. عن تركيب كالي الخاص بك:

قم بتحرير الملف /etc/ssh/sshd_config. ابحث عن سطر `PermitRootLogin without-password` وقم بتغييره لـ `PermitrootLogin yes`.

بدء sshd:

```
root@kali:~# systemctl start ssh
```

تمكين sshd عند الإقلاع:

```
root@kali:~# systemctl enable ssh
```

الآن، يجب أن تكون قادر على الوصول لـ ssh في جهازك كـ root/toor:

```
Host Machine:~ j$ ssh root@192.168.1.12
root@192.168.1.12's password :
The programs included with the Kali GNU/Linux system are free software؛
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  1 21:43:37 2017 from 192.168.1.71
```

الآن يمكننا نقل ملف xz إلى Kali VM. حاول تجنب السحب والإسقاط VM. يمكن أن يسبب مشكلة:

```
scp kali-2017.01-rpi2.img.xz root@192.168.60.185:/root
```

بعد ذلك، ادخل بطاقة SD (بحد أدنى 8 GB) وابحث عن معرف القرص المناسب:

```
root@kali:~# dmesg
[194628.402969] sd 3:0:0:0: Attached scsi generic sg2 type 0
[194628.410035] sd 3:0:0:0: [sdb] 15564800 512-byte logical blocks: (7.97 GB/7.42 GiB)
[194628.410821] sd 3:0:0:0: [sdb] Write Protect is off
[194628.410823] sd 3:0:0:0: [sdb] Mode Sense: 03 00 00 00
[194628.411936] sd 3:0:0:0: [sdb] No Caching mode page found
```

```
[194628.411940] sd 3:0:0:0: [sdb] Assuming drive cache: write through
[194628.420751] sdb: sdb1
```

فك ضغط ملف xz:

```
root@kali:~# cd /root
root@kali:~# unxz kali-2017.01-rpi2.img.xz
```

(بدلاً من ذلك، تحقق من xzcat).

قم بتشغيل أمر **dd** باستخدام معرف القرص الصحيح (dev/sdb/ في حالتنا). تحذير! لا تقم بنسخ هذه القيم ببساطة فقط! بل قم بتغييرها إلى مسار محرك الأقراص الصحيح المطابق لبطاقة SD الخاصة بك.

```
root@kali:~# dd if=/root/kali-2017.01-rpi2.img of=/dev/sdb bs=1M
7000+0 records in
7000+0 records out
7340032000 bytes (7.3 GB, 6.8 GiB) copied, 1356.87 s, 5.4 MB/s
```

ادخل SD الخاصة بك واقلع من Kali Pi الجديد. ستحتاج إلى توصيل HDMI لمعرفة ما يحدث ولوحة مفاتيح USB وفأرة للكتابة والنقر. أي يجب عليك توصيل كابل إيثرنت للحصول على الشبكة (إنه DHCP). أوه، ولا يوجد استماع SSH افتراضياً. ألا تتمنى لو كان لديك المزيد من السيطرة على الأشياء؟ إذن واصل القراءة.

استكشاف Zen-التمرين الرابع، للفصل الرابع - تثبيت KAL Linux ARM المخصص

في التمرين السابق، قمنا بإجراء تثبيت ARM قياسي. كما رأيتم، كانت النتائج أقل من مثيرة. على الرغم من أننا لا نغطي هذا في الكتاب، نعتقد أنه من المهم أن ترى كيفية إنشاء صورة مخصصة. يمكنك ممارسة هذا التمرين على أي جهاز ARM مدعوم، ولكننا سنستخدم Raspberry Pi3. تحقق من قائمة أجهزة ARM المدعومة. سننشئ صورة Kali ARM مخصصة تحتوي على:

- ❖ الحد الأدنى من الحزم.
- ❖ بدون بيئة سطح المكتب (بلا رأس).
- ❖ عنوان IP ثابت على eth0 لذلك لا يتعين علينا البحث عن Pi
- ❖ أدوات مثل `ifconfig` مثبتة.
- ❖ تبدأ خدمة SSH مع الإقلاع، مع تثبيت مفتاح SSH العام مسبقًا.

انطلق، انظر للإجابة. هذا استكشاف، على كل حال.

الإجابة:

قم بتنزيل وتثبيت البرامج النصية للبناء "build scripts"، و build dependencies، و cross compiler.

```
mkdir /root/arm-stuff
cd /root/arm-stuff
```

بعد ذلك، نحتاج لـ cross-compiler لـ armhf. تحتوي هذه الحزمة على إصدارات تم إنشاؤها مسبقًا من Linaro GCC و Linaro GDB ، وهو gdbserver (برنامج يسمح لك بتشغيل GDB على جهاز مختلف عن الجهاز الذي يقوم بتشغيل البرنامج الذي يتم تصحيحه)، وجذر النظام (بجميع الرؤوس و المكتبات لربط البرامج) والتعليمات التي في share/doc:

```
git clone https://gitlab.com/kalilinux/packages/gcc-arm-linux-gnueabihf-4-7
```

سيحتاج كالي للملفات الموجودة في bin/ من أجل للبناء:

```
export PATH=${PATH}:/root/arm-stuff/gcc-arm-linux-gnueabihf-4.7/bin
```

بعد ذلك، السحر الحقيقي. سنأخذ نصوص بناء كالي لينكس ARM. ونستخدمها لإنشاء صورنا الرسمية لـ Kali Linux ARM على http://www.kali.org/downloads.

```
git clone https://gitlab.com/kalilinux/build-scripts/kali-arm
cd ~/arm-stuff/kali-arm-build-scripts
```

بعد ذلك، قم بتثبيت dependencies المطلوبة. هذا سوف يستغرق بضع دقائق:

```
./build-deps.sh
```

بعد ذلك، قم بتحرير البرنامج النصي لبناء ARM، وقم بتغيير الحقول المطلوبة. نقوم بتحرير نص Raspberry Pi3 Kali ARM. يحتوي على nexmon مضمن: إطار تصحيح البرامج الثابتة المستند إلى C لشرائح WiFi من Broadcom/Cypress التي تتيح وضع المراقبة وحقن الإطار والمزيد.

في حالتنا يمكننا إزالة **سطح المكتب**، ومعظم **الأدوات والإضافات**. بالإضافة إلى ذلك، نريد إعداد عنوان Raspberry Pi IP ليكون IP ثابتًا حتى نتمكن من SSH إليه لاحقًا. بالطبع، يجب أن يبدأ SSH في وقت الإقلاع، ولديه مفتاحنا العام.

```
nano rpi3-nexmon.sh
```

أولاً، سنقوم بالتعليق على أقسام **سطح المكتب والإضافات**، وإجراء تغييرات على أقسام **الأدوات والخدمات**:

```
#desktop="fonts-croscore fonts-crosextra-caladea fonts-crosextra-carlito gnome-theme-kali gtk3-engines-xfce kali-desktop-xfce kali-root-login lightdm network-manager network-manager-gnome xfce4 xserver-xorg-video-fbdev xserver-xorg-input-evdev xserver-xorg-input-synaptics"

#tools="aircrack-ng ethtool hydra john libnfc-bin mfoc nmap passing-the-hash sqlmap usbutils winexe wireshark net-tools"

tools="aircrack-ng nmap hostapd"


#services="apache2 openssh-server gnupg"

services="openssh-server gnupg"


#extras="iceweasel xfce4-terminal wpasupplicant python-smbus i2c-tools python-requests python-configobj python-pip"
```

سنقوم أيضًا بإجراء تغييرات على قسم **الحزم**، مع إزالة **سطح المكتب والإضافات**:

```
#packages="${arm} ${base} ${desktop} ${tools}
${services} ${extras}"
packages="${arm} ${base} ${tools} ${services}"
```

أبعد من ذلك، سنقوم بإخراج eth0 من dhcp وتعيين عنوان ثابت:

```
auto eth0
        iface eth0 inet static
        address 192.168.1.12
        netmask 255.255.255.0
        gateway 192.168.1.1
EOF
```

يمكن عرض التغييرات التي أجريناها بطريقة أخرى باستخدام أداة **diff**، التي تقارن الملفات. هنا نرى قبل وبعد. تُظهر الخطوط البيضاء الأسطر التي تتطابق بين الملفات (ولكن تم نقلها في هذه الحالة لأننا أدرجنا بعض الأسطر). تعرض الخطوط الحمراء عمليات الحذف، وتظهر الخطوط الخضراء الإضافات. لاحظ أنه في هذا الاختلاف، قمنا بحذف خطوط التكوين بدلاً من التعليق عليها:

```
root@kali:~/arm-stuff/kali-arm-build-scripts# git diff
diff --git a/rpi3-nexmon-bh.sh b/rpi3-nexmon-bh.sh
index 0afe723..4676e21 100755
--- a/rpi3-nexmon-bh.sh
+++ b/rpi3-nexmon-bh.sh
@@ -25,14 +25,12 @@ TOPDIR=`pwd`

 arm="abootimg cgpt fake-hwclock ntpdate u-boot-tools vboot-utils vboot-kernel-utils"
 base="e2fsprogs initramfs-tools kali-defaults kali-menu parted sudo usbutils"
-desktop="fonts-croscore fonts-crosextra-caladea fonts-crosextra-carlito gnome-theme-kali gtk
work-manager network-manager-gnome xfce4 xserver-xorg-video-fbdev xserver-xorg-input-evdev xs
-tools="aircrack-ng ethtool hydra john libnfc-bin mfoc nmap passing-the-hash sqlmap usbutils
-services="apache2 openssh-server"
-extras="iceweasel xfce4-terminal wpasupplicant python-smbus i2c-tools python-requests python
+tools="aircrack-ng nmap hostapd"
+services="openssh-server"
 # kernel sauces take up space yo.
 size=7000 # Size of image in megabytes

-packages="${arm} ${base} ${desktop} ${tools} ${services} ${extras}"
+packages="${arm} ${base} ${tools} ${services}"
 architecture="armhf"
 # If you have your own preferred mirrors, set them here.
 # After generating the rootfs, we set the sources.list to the default settings.
@@ -73,7 +71,10 @@ auto lo
 iface lo inet loopback

 auto eth0
-iface eth0 inet dhcp
+       iface eth0 inet static
+       address 192.168.1.12
+       netmask 255.255.255.0
+       gateway 192.168.1.1
 EOF
```

بمجرد إجراء التغييرات، يمكننا تشغيل البرنامج النصي للبناء بمعرف أنيق (1.0" a lame" في هذا المثال). لاحظ أن هذا قد يستغرق أكثر من ساعة، بناءً على وحدة المعالجة المركزية والذاكرة والنطاق الترددي:

```
./rpi3-nexmon.sh 1.0
```

بمجرد الانتهاء من ذلك، يجب أن يكون لديك ثلاثة ملفات:

root@kali:~/arm-stuff/kali-arm-build-scripts# **ls -l rpi3-nexmon-bh-1.0/**

```
total 553496
-rw-r--r-- 1 root root        91 Aug  5 12:14 kali-1.0-rpi3-nexmon.img.sha256sum
-rw-r--r-- 1 root root 566765348 Aug  5 12:23 kali-1.0-rpi3-nexmon.img.xz
-rw-r--r-- 1 root root        94 Aug  5 12:23 kali-1.0-rpi3-nexmon.img.xz.sha256sum
```

الآن، يمكنك حرق ISO إلى SD لاختبار الصورة. كما هو الحال دائمًا، تأكد من تحديد معرف الجهاز الصحيح. في حالتنا، dev/sdb/. يمكن أن يستغرق ذلك 20 دقيقة أو أكثر، عند تشغيله من جهاز افتراضي تم تكوينه بشكل صحيح:

```
root@kali:~# cd /root/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0/

root@kali:~/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0# ls

kali-1.0-rpi3-nexmon.img.sha256sum kali-1.0-rpi3-nexmon.img.xz kali-1.0-rpi3-nexmon.img.xz.sha256sum

root@kali:~/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0# xzcat kali-1.0-rpi3-nexmon.img.xz | dd of=/dev/sdb bs=1M
```

بعد ذلك، قم بتشغيل Kali Pi. يجب أن تجده على 192.168.1.12، ويجب أن يكون ssh مفتوحًا. أوه، ومكافأة! **ifconfig** يعمل!

استكشاف Zen - التمرين الخامس ، للفصل الرابع - كالي لينكس ARM chroot

إذا كان البناء الذي صنعته لم يكن مناسبا. لحسن الحظ أنه يمكنك تغييره. في هذا المثال، لنفترض أنك نسيت تثبيت بعض الحزم، مثل net-tools و dnsmasq و mlocate. بدلاً من إعادة تثبيت الجهاز وإعادة تصويره، قم بالتبديل إلى بطاقة RPi3 SD من جهاز Kali الخاص بك وقم بإجراء التغييرات المطلوبة.

نظراً لأن هذا هو دليل تفصيلي، ولم يتم تناوله في الكتاب، فاستمر وانظر للإجابة واكتشف.

الإجابة:

ستبدأ ببطاقة SD من تمرين سابق. في هذا المثال، نستخدم الصورة من التمرين السابق (التمرين الرابع) - بناءنا المخصص. أولاً، قم بتثبيت أدوات الترجمة بواسطة **qemu** والأدوات ذات الصلة في كالي:

```
apt-get install qemu qemu-user qemu-user-static
```

دعنا نقوم بإنشاء مجلد mnt/sd/ للحفاظ على المجلدات التي نعمل عليها منظمة:

```
mkdir /mnt/sd
```

احصل على تعيين محرك الأقراص dev/sd/ بإدخال بطاقة SD الخاصة بـ Pi (هي dev/sdc/). محول USB-SD الخاص بك يحدث فرقا. سنلتقط جميع حوامل محرك الأقراص الفعلية في لقطة واحدة.

```
root@kali:~# mount /dev/sdc2 /mnt/sd/
root@kali:~# ls -l /mnt/sd
total 88
drwxr-xr-x  2 root root  4096 Aug  5 11:36 bin
drwxr-xr-x  2 root root  4096 Jul 18 03:08 boot
drwxr-xr-x  4 root root  4096 Aug  5 11:15 dev
drwxr-xr-x 71 root root  4096 Mar  1 16:43 etc
drwxr-xr-x  2 root root  4096 Jul 18 03:08 home
drwxr-xr-x 13 root root  4096 Aug  5 12:11 lib
drwx------  2 root root 16384 Aug  5 11:39 lost+found
drwxr-xr-x  2 root root  4096 Aug  5 11:15 media
drwxr-xr-x  2 root root  4096 Aug  5 11:15 mnt
drwxr-xr-x  2 root root  4096 Aug  5 11:15 opt
drwxr-xr-x  2 root root  4096 Jul 18 03:08 proc
```

```
drwx------  2 root root  4096 Mar  1 16:43 root
drwxr-xr-x  4 root root  4096 Aug  5 11:15 run
drwxr-xr-x  2 root root  4096 Aug  5 11:36 sbin
drwxr-xr-x  2 root root  4096 Aug  5 11:15 srv
drwxr-xr-x  2 root root  4096 Jul 18 03:08 sys
drwxrwxrwt  7 root root  4096 Mar  1 18:40 tmp
drwxr-xr-x 10 root root  4096 Aug  5 11:15 usr
drwxr-xr-x 11 root root  4096 Aug  5 11:15 var
```

هل لاحظت كيف يتم الآن تعيين جميع مجلدات بطاقة SD الخاصة بـ Raspberry Pi على نظامك في /mnt/sd؟

قم بتحميل جميع "أنظمة الملفات الخاصة" في /mnt/sd. لاحظ أننا سنلغي خيارات التثبيت من /etc/fstab على بعض الخرائط التي تم تعيينها بالفعل مع الخيار **o**-:

```
mount -t proc none /mnt/sd/proc
mount -t sysfs none /mnt/sd/sys
mount -o bind /dev /mnt/sd/dev
mount -o bind /dev/pts /mnt/sd/dev/pts
```

دعونا نسحب أدوات تجميع emu. نحتاج إليها لتجميع عناصر ARM لأن هدفنا هو ARM!

```
cp /usr/bin/qemu-arm-static /mnt/sd/usr/bin
```

حان الوقت للدخول chroot! بمجرد الدخول إلى chroot، ستفترض جميع الإشادات التي ننفذها أن mnt/sd/ هو نظام ملفات الجذر الخاص بنا. إنها خدعة رائعة. لاحظ أننا قمنا بتعيين LAN=C لمنع التحذيرات المحلية في chroot الخاص بك:

```
LANG=C chroot /mnt/sd/
```

دعونا نجري بعض التغييرات على نظام ملفات Pi. هذا هو الجزء الرائع. كل هذا يحدث على نظام ملفات Pi الخاص بك!

```
# apt-get update
# apt-get install mlocate
# apt-get install net-tools
# apt-get install hostapd dnsmasq
```

تابع التكوين حسب الضرورة. بمجرد الانتهاء، اخرج من chroot وقم بإلغاء تحميل بطاقة SD.

```
root@kali:~# exit
```

نحتاج إلى إلغاء وصل كل المجلدات التي قمنا بوصلها (أو تثبيتها):

```
umount /mnt/sd/dev/pts
umount /mnt/sd/dev/
umount /mnt/sd/sys
umount /mnt/sd/proc
umount /mnt/sd
```

أخيرًا، أدخل بطاقة SD في Pi، وابدأ!

اختبار KLCP للفصل الرابع

١. ما هو التكوين الموصى به لخادم Kali SSH البسيط القائم على Intel بدون سطح مكتب (بلا رأس)؟

- 4096 MB RAM / 40 GB hard drive free space / i386 CPU
- 128 MB RAM / 1 GB hard drive free space / arm64 CPU
- 512 MB RAM / 2 GB hard drive free space / amd64 CPU
- 2048 MB RAM / 20 GB hard drive free space / SPARC CPU

٢. بشكل عام، أي من هذه ليست متطلبات الحد الأدنى لسطح المكتب كالي لينكس؟

- 4096 MB RAM / 40 GB hard drive free space
- 128 MB RAM / 1 GB hard drive free space
- 512 MB RAM / 2 GB hard drive free space
- 2048 MB RAM / 20 GB hard drive free space

٣. صح أو خطأ: سيفشل تثبيت Kali Linux إذا لم تختار مرآة للشبكة.

- صح
- خطأ

٤. صح أو خطأ: عند الإقلاع من mini.iso، سيفشل تثبيت Kali Linux إذا تعذر الكشف عن أجهزة الشبكة.

- صح
- خطأ

٥. ما هو نظام التقسيم الذي من المرجح أن يتأثر بخطأ المستخدم؟

- Guided – use entire Disk
- Guided – use entire disk and set up LVM
- Manual
- Guided – use entire disk and set up encrypted LVM

٦. ما هي طريقة التقسيم المفضلة للخوادم والأنظمة متعددة المستخدمين؟

- Separate /home, /var, and /tmp partitions
- Separate /home/ partition
- All files in one partition
- No Partitions

٧. سيؤدي تثبيت إصدار حديث من Windows بعد تثبيت Kali إلى:

- فشل بسبب تثبيت محمل الإقلاع السابق
- مسح محمل الإقلاع ومنع كالي من الإقلاع
- مسح كالي لينكس
- إنشاء إقلاع آمن للفشل لنظام كالي

٨. ما هو الغرض من preseed.cfg؟

- o تعيين seed عشوائي لوظائف التشفير
- o إنشاء افتراضيات معقولة لمعظم إعدادات المستخدم
- o ملف التكوين الخاص بالبرنامج الخفي
- o توفير إجابات محددة مسبقًا لأسئلة التثبيت

٩. ما هو الإجراء الأبسط والأكثر فعالية لتثبيت كالي على جهاز ARM؟

- o استخدم الإنشاء المباشر "live-build" لإنشاء ملف ISO يستند على ARM
- o استخدم mini.iso لإنشاء نظام أساسي، ثم قم بتشغيل `apt-get update`
- o الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها واتبع خطوات التثبيت
- o الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها وتسجيل الدخول باستخدام root/toor

١٠. ما الطريقة التي لا تتوفر بسهولة لحفظ سجلات تصحيح الأخطاء أثناء التثبيت الفاشل؟

- o التخزين على القرص المرن
- o حفظ السجلات على kali bug tracker
- o عرض السجلات من خادم ويب
- o حفظ السجلات لنظام ملفات موصول

الإجابات:

1. 512 MB RAM / 2 GB hard drive free space / amd64 CPU
2. 512 MB RAM / 2 GB hard drive free space

٣. خطأ

٤. صح

5. Manual
6. Separate /home, /var, and /tmp partitions

٧. مسح محمل الإقلاع ومنع كالي من الإقلاع

٨. توفير إجابات محددة مسبقًا لأسئلة التثبيت

٩. الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها وتسجيل الدخول باستخدام root/toor

١٠. حفظ السجلات على kali bug tracker

---((الفصل الخامس))---

في هذا الفصل، سنلقي نظرة على طرق مختلفة يمكنك من خلالها تكوين Kali Linux.

أولاً، في القسم 1.5، "تكوين الشبكة"، سنوضح لك كيفية تكوين إعدادات الشبكة باستخدام البيئة الرسومية وبيئة سطر الأوامر.

في القسم 2.5 "إدارة مستخدمي Unix ومجموعات Unix"، سنتكلم عن المستخدمين والمجموعات، ونوضح لك كيفية إنشاء وتعديل حسابات المستخدمين، وتعيين كلمات المرور، وتعطيل الحسابات، وإدارة المجموعات.

أخيرًا، سنناقش الخدمات في القسم 3.5، "تكوين الخوادم" وسنشرح كيفية إعداد الخدمات العامة والمحافظة عليها، ونركز أيضًا على الثلاث الخدمات المهمة للغاية وهي : SSH و PostgreSQL و Apache.

الإختصارا الواردة في هذا الفصل:

(SSH: **S**ecure **Sh**ell**)**, **(Gnome**: **G**NU **N**etwork **O**bject **M**odel **E**nvironment**)**

(GNU: **G**nu **N**ot **U**nix**)**, **(**Unix: ليس اختصارا**)**, **(IP**: **I**nternet **P**rotocol**)**

(Dhcp: **D**ynamic **H**ost **C**onfiguration **P**rotocol**)**

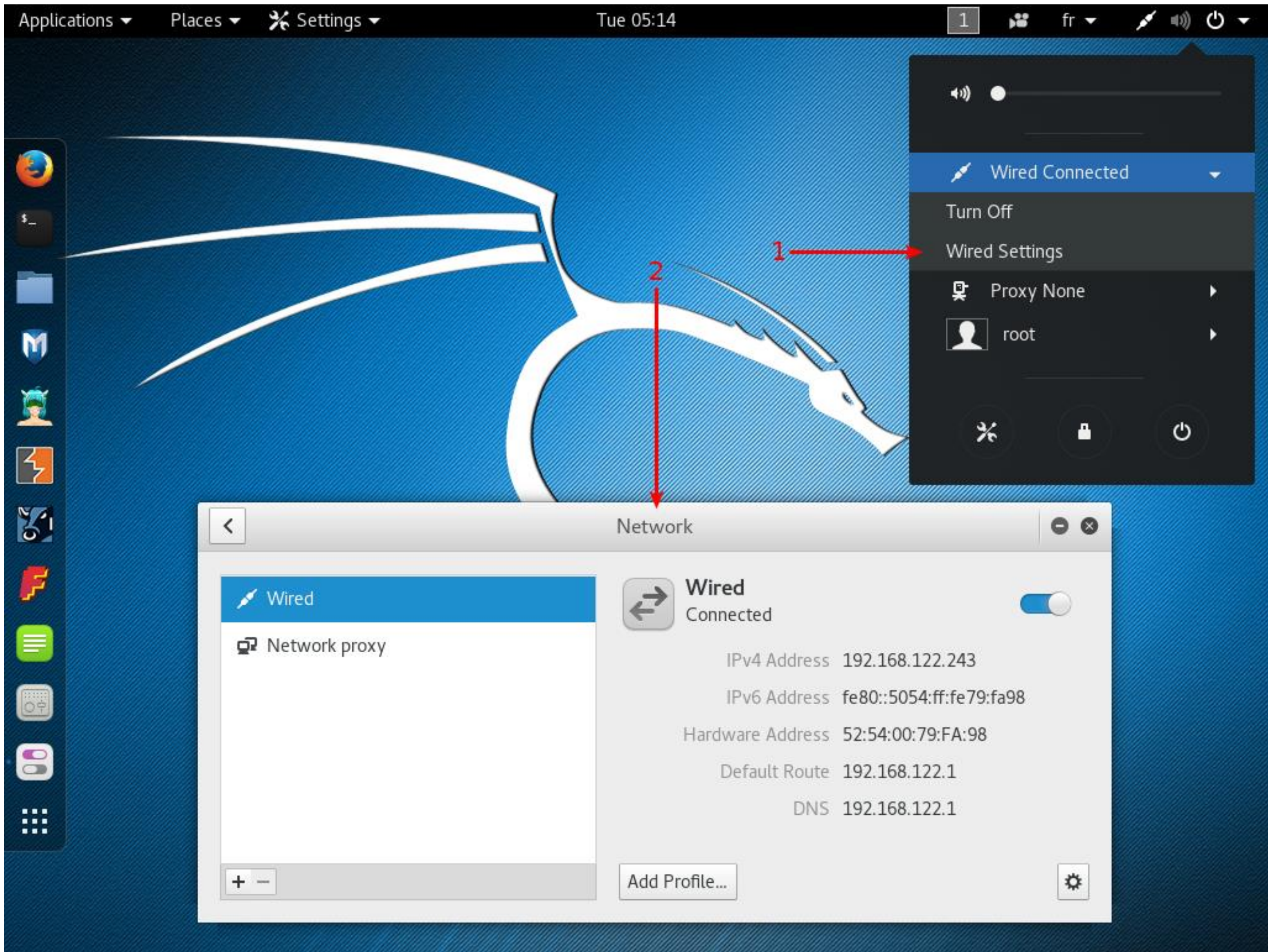
(MAC: **M**edia **A**ccess **C**ontrol**)**, **(SSID: S**ervice **S**et **ID**entifier**)**

(DNS: **D**omain **N**ame **S**ystem**)**, **(PPTP: P**oint-to-**P**oint **T**unneling **P**rotocol**)**.

1.5. تكوين الشبكة

١.١.٥. على سطح المكتب مع NetworkManager

في التثبيت العادي لسطح المكتب، سيكون لديك مدير شبكة -NetworkManager- مثبتاً بالفعل ويمكن التحكم فيه وتكوينه من خلال مركز التحكم في GNOME ومن خلال القائمة العلوية اليمنى كما هو موضح في الشكل .1.5 "شاشة تكوين الشبكة".



في شكل .1.5 "شاشة تكوين الشبكة".

يعتمد التكوين الافتراضي للشبكة على DHCP للحصول على عنوان IP وخادم DNS والبوابة، ولكن يمكنك استخدام رمز الترس في الزاوية اليمنى السفلية لتغيير التكوين بعدة طرق (على سبيل المثال: تعيين عنوان MAC والتبديل إلى إعداد static، قم بتمكين أو تعطيل IPv6، وإضافة

موجهات "رواتر"). يمكنك إنشاء ملفات تعريف لحفظ تكوينات شبكة سلكية متعددة والتبديل بينها بسهولة. بالنسبة للشبكات اللاسلكية، ترتبط إعداداتها تلقائيًا بمعرفها العام (SSID).

يعالج NetworkManager أيضًا الاتصالات عن طريق (الشبكة اللاسلكية واسعة النطاق "Wireless Wide Area Network" WWAN) وعن طريق أجهزة المودم باستخدام بروتوكول نقطة إلى نقطة عبر إيثرنت (PPPOE). أخيرًا وليس آخرًا، يوفر التكامل مع العديد من أنواع الشبكات الخاصة الافتراضية (VPN) من خلال المكونات الإضافية المخصصة: SSH و OpenVPN و Cisco's VPNC و PPTP و Strongswan.

حزم *-network-manager، معظمها غير مثبتة افتراضياً.

لاحظ أنك تحتاج إلى الحزم الملحقة بـ gnome- لتتمكن من تكوينها من خلال واجهة المستخدم الرسومية.

2.1.5. بسطر الأوامر باستخدام حزم ifupdown

بدلاً من ذلك، عندما تفضل عدم استخدام (أو لا يمكنك الوصول إلى) سطح مكتب رسومي، يمكنك تكوين الشبكة عن طريق حزمة ifupdown المثبتة بالفعل، والتي تتضمن أدوات **ifup** و**ifdown**. تقوم هذه الأدوات بقراءة التعريفات من ملف التكوين **/etc/network/interfaces** والتي هي في صميم البرنامج النصي **/etc/init.d/networking** الذي يقوم بتكوين الشبكة في وقت الإقلاع.

يمكن إلغاء تكوين كل أجهزة الشبكة التي تتم إدارته بواسطة ifupdown في أي وقت باستخدام **ifdown** *network-device*. يمكنك بعد ذلك تعديل **/etc/network/interfaces** وإعادة عمل الشبكة احتياطياً (مع التكوين الجديد) باستخدام **ifup** *network-device*.

دعنا نلقي نظرة على ما يمكننا وضعه في ملف تكوين ifupdown. هناك توجيهان رئيسيان: **auto** *network-device*: الذي يخبر عن إعادة تهيئة لتكوين واجهة الشبكة تلقائيًا بمجرد توفرها. **iface** *network-device inet/inet6 type*: لتكوين واجهة معينة. على سبيل المثال، يبدو تكوين DHCP العادي كما يلي:

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet dhcp

لاحظ أن التكوين الخاص لجهاز الاسترجاع (loopback) يجب أن يكون موجودًا دائمًا في هذا الملف. لتكوين عنوان IP ثابت، يجب عليك تقديم المزيد من التفاصيل مثل عنوان IP والشبكة وعنوان IP الخاص بالبوابة:

```
auto eth0

iface eth0 inet static

address 192.168.0.3

netmask 255.255.255.0

broadcast 192.168.0.255

network 192.168.0.0

gateway 192.168.0.1
```

بالنسبة للواجهات اللاسلكية، يجب أن يكون لديك حزمة wpasupplicant (مضمنة في Kali افتراضيًا)، والتي توفر العديد من خيارات **wpa-*** التي يمكن استخدامها في **/etc/network/interfaces.** ألق نظرة على /usr/share/doc/wpasupplicant/README.Debian.gz للحصول على أمثلة وشروحات. أكثر الخيارات شيوعًا هي: wpa-ssid (الذي يحدد اسم الشبكة اللاسلكية للانضمام).

و wpa-psk (الذي يحدد كلمة المرور أو المفتاح الذي يحمي الشبكة).

iface wlan0 inet dhcp

wpa-ssid *MyNetWork*

wpa-psk *plaintextsecret*

3.1.5. على سطر الأوامر باستخدام *systemd-networkd*

على الرغم من أن *ifupdown* هي الأداة التاريخية لدبيان، ولكنها لا تزال هي الأداة الافتراضية للخادم أو أي تثبيتات أخرى بسيطة، إلا أن هناك أداة أحدث تستحق التجربة وهي : *systemd-networkd*. ودمجها مع نظام init *systemd* يجعلها خيارًا جذابًا للغاية. لا يقتصر الأمر على التوزيعات المستندة على دبيان (على عكس *ifupdown*) وقد تم تصميمه ليكون صغيرًا جدًا وفعالًا وسهل التكوين نسبيًا إذا فهمت بنية ملفات وحدة النظام. يعد هذا خيارًا جذابًا بشكل خاص إذا كنت تعتقد أنه يصعب تهيئة *NetworkManager*.

يمكنك تكوين **systemd-networkd** عن طريق وضع ملفات **network**. في المجلد **/etc/systemd/network/**. بدلاً من ذلك، يمكنك استخدام **/lib/systemd/network/** لملفات الحزم أو **/run/systemd/network/** للملفات التي تم إنشاؤها في وقت التشغيل. تم توثيق تنسيق هذه الملفات في systemd.network(5). يشير قسم **Match** إلى واجهات الشبكة التي ينطبق عليها التكوين. يمكنك تحديد الواجهة بعدة طرق، بما في ذلك عن طريق عنوان التحكم في الوصول إلى الوسائط (MAC) أو نوع الجهاز. يحدد قسم **Network** تكوين الشبكة.

مثال 1.5 التكوين الثابت في **/etc/systemd/network/50-static.network**

```
[Match]

Name=enp2s0

[Network]

Address=192.168.0.15/24

Gateway=192.168.0.1

DNS=8.8.8.8
```

مثال 2.5 التكوين المستند على DHCP في **etc/systemd/network/80-/dhcp.network**

```
[Match]
Name=en*
[Network]
DHCP=yes
```

لاحظ أنه تم تعطيل **system-networkd** بشكل افتراضي، لذلك إذا كنت ترغب في استخدامه، يجب عليك تمكينه. يعتمد أيضًا على **systemd-resolved** من أجل التكامل الصحيح لدقة DNS، الأمر الذي يتطلب منك استبدال ملف **etc/resolv.conf/** بوصله رمزية لـ **run/system/resolve/resolv.conf/**، والذي تم إدارته بواسطة **systemd-resolved**.

```
systemctl enable systemd-networkd
systemctl enable systemd-resolved
systemctl start systemd-networkd
systemctl start systemd-resolved
ln -sf /run/system/resolve/resolv.conf /etc/resolv.conf
```

على الرغم من أن **systemd-networkd** يعاني من بعض القيود، مثل عدم وجود دعم متكامل للشبكات اللاسلكية، يمكنك الاعتماد على تكوين **wpa_supplicant** خارجي موجود مسبقًا للدعم اللاسلكي. ومع ذلك، فهي مفيدة بشكل خاص في الـ containers والآلات الافتراضية "virtual machines"والتي تم تطويرها في الأصل للبيئات التي تعتمد فيها تهيئة شبكة الـ containers على تكوين شبكة مضيفها. في هذا السيناريو، يسهل **systemd-networkd** إدارة كلا الجانبين بطريقة منسقة مع الاستمرار في دعم جميع أنواع أجهزة الشبكة الافتراضية التي قد تحتاجها في هذا النوع من السيناريو انظر (5)systemd.netdev.

2.5. إدارة مستخدمي Unix ومجموعات Unix

تتكون قاعدة بيانات مستخدمي ومجموعات يونكس من ملفات نصية **/etc/passwd** (قائمة المستخدمين)، **/etc/shadow** (كلمات مرور مشفرة للمستخدمين)، **/etc/group** (قائمة المجموعات)، و **/etc/gshadow** (كلمات مرور مشفرة للمجموعات). تنسيقاتها موثقة في passwd (5) و shadow (5) و group (5) و gshadow (5) على التوالي. بينما يمكن تحرير هذه الملفات يدويًا باستخدام أدوات مثل **vipw** و **vigr**، هناك أدوات ذات مستوى أعلى لإجراء العمليات الأكثر شيوعًا.

استخدام getent لاستشارة قاعدة بيانات المستخدم

يتحقق الأمر **getent** (get entries) من قواعد بيانات النظام (بما في ذلك قواعد البيانات الخاصة بالمستخدمين والمجموعات) باستخدام وظائف المكتبة المناسبة، والتي بدورها تستدعي وحدات خدمة تبديل الاسم (NSS) المكونة في الملف /etc/nsswitch.conf. يأخذ الأمر مدخل أو اثنتين: اسم قاعدة البيانات للتحقق، ومفتاح بحث محتمل. وبالتالي، فإن الأمر **getent passwd** kaliuser1 سيعيد المعلومات من قاعدة بيانات المستخدم المتعلقة بالمستخدم kaliuser1.

```
root@kali:~# getent passwd kaliuser1
kaliuser1:x:1001:1001:Kali User,4444,123-867-5309,321-867-5309:/home/kaliuser1:/bin/bash
```

١.٢.٥. إنشاء حسابات المستخدمين

قد تحتاج أحيانا إلى إنشاء حسابات لأسباب مختلفة، خاصة إذا كنت تستخدم Kali كنظام تشغيل أساسي. الطريقة الأكثر شيوعًا لإضافة مستخدم هي الأمر **adduser**، الذي يطلب مدخل مطلوب وهو: اسم المستخدم؛ للمستخدم الجديد الذي ترغب في إنشائه.

يطرح أمر **adduser** بعض الأسئلة قبل إنشاء الحساب ولكن استخدامه واضح إلى حد ما. يتضمن ملف التكوين الخاص به، **/etc/adduser.conf**، العديد من الإعدادات المثيرة للاهتمام. يمكنك، على سبيل المثال، تحديد نطاق معرفات المستخدم (UIDs) التي يمكن استخدامها، وإملاء ما إذا كان المستخدمون يشتركون في مجموعة مشتركة أم لا، وتحديد الصدفات الافتراضية، والمزيد.

يؤدي إنشاء حساب إلى تشغيل محتوى المجلد الرئيسي للمستخدم بمحتويات النموذج **/etc/skel/**. يوفر ذلك للمستخدم مجموعة من المجلدات القياسية وملفات التكوين.

في بعض الحالات، سيكون من المفيد إضافة مستخدم إلى مجموعة (بخلاف المجموعة الرئيسية الافتراضية) لمنح أذونات إضافية. على سبيل المثال، المستخدم الذي تم تضمينه في مجموعة *sudo* لديه امتيازات إدارية كاملة من خلال الأمر **sudo**. يمكن تحقيق ذلك باستخدام أمر مثل: **adduser** *user group*.

٢.٢.٥. تعديل حساب موجود أو كلمة مرور

تسمح الأوامر التالية بتعديل المعلومات المخزنة في حقول محددة من قواعد بيانات المستخدم:

passwd - يسمح للمستخدم العادي بتغيير كلمة المرور الخاصة به، والتي بدورها تقوم بتحديث ملف **/etc/shadow**. || أو كلمة مرور مستخدم أخر، مثلا: sudo passwd *username*||

chfn– (change full name) ، المحجوز للمستخدم الفائق (الجذر)، يعدل حقل **GECOS**، أو حقل "معلومات عامة".

chsh – (change shell) يغير واجهة تسجيل دخول المستخدم. ومع ذلك، ستقتصر الخيارات المتاحة على تلك المدرجة في **/etc/shells**؛ المسؤول، من ناحية أخرى، غير ملزم بهذا التقييد ويمكنه تعيين shell لأي برنامج تم اختياره.

chage – (change age) يسمح للمسؤول بتغيير إعدادات انتهاء صلاحية كلمة المرور بتمرير اسم المستخدم كمدخل أو سرد الإعدادات الحالية باستخدام الخيار user **-l**. بدلاً من ذلك، يمكنك أيضًا فرض انتهاء صلاحية كلمة المرور باستخدام الأمر **passwd -e** user، مما يجبر المستخدم على تغيير كلمة المرور الخاصة به في المرة التالية التي يقوم فيها بتسجيل الدخول.

٣.٢.٥. تعطيل حساب

قد تجد نفسك بحاجة إلى تعطيل حساب (حظر مستخدم) كإجراء تأديبي، لأغراض التحقيق، أو ببساطة في حالة الغياب المطول أو النهائي للمستخدم. يعني الحساب المعطل أن المستخدم لا يمكنه تسجيل الدخول أو الوصول إلى الجهاز. يظل الحساب كما هو على الجهاز ولا يتم حذف أي ملفات أو بيانات؛ ببساطة لا يمكن الوصول إليها. يتم تحقيق ذلك باستخدام الأمر **passwd** *user* **-l** (القفل "lock"). تتم إعادة تمكين الحساب بطريقة مماثلة، مع الخيار **-u** (إلغاء القفل).

--||--

لقفل الحساب: passwd -l *user*

لإلغاء قفل الحساب: passwd --unlock *user*

لحذف كلمة المرور: passwd --delete *user*

وغيره .. تحقق من man passwd وانظر للخيارات المتاحة.

--||--

٤.٢.٥. إدارة مجموعات يونكس

يضيف الأمر **addgroup** مجموعة و **delgroup** يحذف مجموعة، يعدل الأمر **groupmod** معلومات المجموعة (رقم تعريفها **gid**- أو معرفها). يقوم الأمر **gpasswd** *group* بتغيير كلمة مرور المجموعة، بينما يقوم الأمر **gpasswd -r** *group* بحذفها.

العمل على عدة مجموعات

قد يكون كل مستخدم عضوا في العديد من المجموعات. يتم إنشاء المجموعة الرئيسية للمستخدم بشكل افتراضي أثناء التكوين الأولي للمستخدم. بشكل افتراضي، ينتمي كل ملف ينشئه المستخدم إلى المستخدم وكذلك إلى المجموعة الرئيسية للمستخدم. هذا ليس مرغوبًا دائمًا؛ على سبيل المثال، عندما يحتاج المستخدم للعمل في مجلد مشترك من قبل مجموعة غير مجموعته الرئيسية. في هذه الحالة، يحتاج المستخدم إلى تغيير المجموعات باستخدام أحد الأوامر التالية: **newgrp**، الذي يبدأ بصدفة جديدة، أو **sg**، والذي يقوم ببساطة بتنفيذ أمر باستخدام المجموعة البديلة المزودة. تسمح هذه الأوامر أيضًا للمستخدم بالانضمام إلى مجموعة لا ينتمي إليها حاليًا. إذا كانت المجموعة محمية بكلمة مرور، فسوف تحتاج إلى توفير كلمة المرور المناسبة قبل تنفيذ الأمر.

بدلاً من ذلك، يمكن للمستخدم تعيين بت **setgid** في المجلد، مما يؤدي إلى أن تنتمي الملفات التي تم إنشاؤها في هذا المجلد تلقائيًا إلى المجموعة الصحيحة.

يعرض الأمر **id** الحالة الحالية للمستخدم، مع معرفه الشخصي (متغير uid)، والمجموعة الرئيسية الحالية (متغير gid)، وقائمة المجموعات التي ينتمون إليها (متغير groups).

٣.٥. تكوين الخدمات

في هذا القسم، سنلقي نظرة على الخدمات (تسمى أحيانًا daemons)، أو البرامج التي تعمل كعمليات في الخلفية وتؤدي وظائف متنوعة للنظام. سنبدأ بمناقشة ملفات التكوين وسنشرع في شرح كيفية عمل بعض الخدمات المهمة (مثل SSH وPostgreSQL وApache) وكيف يمكن تكوينها.

١.٣.٥. تكوين برنامج معين

عندما تريد تكوين حزمة غير معروفة، يجب عليك متابعة هذه المراحل. أولاً، يجب عليك قراءة ما وثقه مشرف الحزمة. يعد ملف **/usr/share/doc/***package***/README.Debian** مكانًا جيدًا للبدء. غالبًا ما يحتوي هذا الملف على معلومات حول الحزم، بما في ذلك المؤشرات التي قد تحيلك إلى وثائق أخرى. غالبًا ما توفر لك الكثير من الوقت، وتجنب الكثير من الإحباط، من خلال قراءة هذا الملف أولاً لأنه غالبًا ما يوضح تفاصيل الأخطاء والحلول الأكثر شيوعًا لمعظم المشاكل الشائعة.

بعد ذلك، يجب عليك إلقاء نظرة على الوثائق الرسمية للبرنامج. راجع القسم ١.٦. "مصادر التوثيق" للحصول على نصائح حول كيفية العثور على مصادر توثيق مختلفة. يعطي الأمر:

dpkg -L *package*

قائمة بالملفات المضمنة في الحزمة؛ لذلك يمكنك تحديد الوثائق المتاحة بسرعة (بالإضافة إلى ملفات التكوين الموجودة في /etc/). أيضًا الأمر: **dpkg -s** *package* يعرض البيانات الوصفية للحزمة وتعرض أي حزم ممكنة موصى بها أو مقترحة؛ هناك، يمكنك العثور على وثائق أو أداة مساعدة من شأنها تسهيل تكوين البرنامج.

أخيرًا، غالبًا ما يتم توثيق ملفات التكوين ذاتيًا من خلال العديد من التعليقات التفسيرية التي توضح بالتفصيل مختلف القيم الممكنة لكل إعداد تكوين. في بعض الحالات، يمكنك الحصول على البرنامج وتشغيله عن طريق إلغاء تعليق سطر واحد فقط في ملف التكوين. في حالات أخرى، يتم توفير أمثلة لملفات التكوين في المجلد **/usr/share/doc/*package*/examples/**. قد تكون بمثابة أساس لملف التكوين الخاص بك.

٢.٣.٥. تكوين SSH لتسجيلات الدخول عن بعد

يسمح لك SSH بتسجيل الدخول إلى الجهاز عن بُعد أو نقل الملفات أو تنفيذ الأوامر. الأداة القياسية هي (ssh) وأما الخدمة (sshd) للاتصال بالأجهزة عن بعد.

أثناء تثبيت حزمة opensh-server افتراضيًا، يتم تعطيل خدمة SSH افتراضيًا وبالتالي لا يتم تشغيلها في وقت الإقلاع. يمكنك بدء تشغيل خدمة SSH يدويًا بكتابة الأمر:

```
systemctl start ssh
```

أو تهيئتها للبدء في وقت الإقلاع باستخدام الأمر:

```
systemctl enable ssh
```

خدمة SSH لها تكوين افتراضي معقول نسبيًا، ولكن نظرًا لقدراتها القوية وطبيعتها الحساسة، من الجيد معرفة ما يمكنك القيام به في ملف التكوين الخاص بها، **/etc/ssh/sshd_config**. تم توثيق جميع الخيارات في (5) sshd_config.

يعطل التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى كلمة المرور للمستخدم الجذر، مما يعني أنه يجب عليك أولاً إعداد مفاتيح SSH باستخدام **ssh-keygen**. يمكنك تمديد هذا إلى جميع المستخدمين عن طريق تعيين **PasswordAuthentication** إلى **no**، أو يمكنك رفع هذا القيد عن طريق تغيير **PermitRootLogin** إلى **yes** (بدلاً من كلمة المرور المحظورة الافتراضية). تستمع خدمة SSH بشكل افتراضي على المنفذ (port) 22 ولكن يمكنك تغيير ذلك باستخدام توجيه **Port**.

لتطبيق الإعدادات الجديدة، يجب كتابة الأمر **systemctl reload ssh**.

توليد مفاتيح مضيف SSH جديدة

يحتوي كل خادم SSH على مفاتيح التشفير الخاصة به؛ يتم تسميتها "مفاتيح مضيف SSH" ويتم تخزينها في /etc/ssh/ssh_host_*. يجب الحفاظ على خصوصيتها إذا كنت تريد السرية ولا يجب مشاركتها مع أجهزة متعددة.

عندما تقوم بتثبيت النظام الخاص بك عن طريق نسخ صورة قرص كاملة (بدلاً من استخدام برنامج debian-installer)، فقد تحتوي الصورة على مفاتيح مضيف SSH تم إنشاؤها مسبقًا والتي يجب عليك استبدالها بمفاتيح تم إنشاؤها حديثًا. من المحتمل أن تأتي الصورة أيضًا بكلمة مرور جذر افتراضية تريد إعادة تعيينها في نفس الوقت. يمكنك القيام بكل ذلك باستخدام الأوامر التالية:

```
#passwd [...]
#rm /etc/ssh/ssh_host*_
#dpkg-reconfigure openssh-server
#service ssh restart
```

٣.٣.٥. تكوين قواعد بيانات PostgreSQL

PostgreSQL هو خادم قاعدة بيانات. نادرًا ما يكون مفيدًا من تلقاء نفسه ولكن يتم استخدامه من قبل العديد من الخدمات الأخرى لتخزين البيانات. ستصل هذه الخدمات بشكل عام إلى خادم قاعدة البيانات عبر الشبكة وتتطلب عادة بيانات اعتماد المصادقة لتكون قادرة على الاتصال. وبالتالي يتطلب إعداد هذه الخدمات إنشاء قواعد بيانات PostgreSQL وحسابات المستخدمين مع الامتيازات المناسبة لقاعدة البيانات. حتى نتمكن من القيام بذلك، نحتاج إلى تشغيل الخدمة، لذا دعنا نبدأ بالأمر:

```
systemctl start postgresql
```

دعم العديد من إصدارات PostgreSQL

تسمح حزمة PostgreSQL بتثبيت نسخ متعددة من خادم قاعدة البيانات. من الممكن أيضًا التعامل مع *clusters* متعددة (cluster هي مجموعة من قواعد البيانات التي يقدمها نفس مدير البريد "postmaster"). لتحقيق ذلك، يتم تخزين ملفات التكوين في /etc/postgresql/*version*/*cluster-name*/.

من أجل تشغيل الـ clusters جنبًا إلى جنب، يتم تعيين رقم المنفذ التالي المتاح لكل مجموعة جديدة (عادةً ٥٤٣٣ للمجموعة الثانية). ملف postgresql.service عبارة عن صدفة فارغة، مما يجعل من السهل العمل على كل المجموعات "clusters" معًا حيث أن لكل مجموعة وحدتها الخاصة (postgresql@*version*-*cluster*.service).

٥.٣.٣.١. نوع الاتصال ومصادقة العميل

بشكل افتراضي، يستمع PostgreSQL للاتصالات الواردة بطريقتين: على منفذ TCP 5432 لواجهة المضيف المحلي وعلى المقبس " socket" المستند للملفات **/var/run/postgresql/.s.PGSQL.5432**. يمكن تكوين ذلك في **postgresql.conf** مع توجيهات متنوعة: **listen_addresses** للعنوان الذي تريد الاستماع منه، **port** لمنفذ TCP، و **unix_socket_directories** لتعريف المجلد حيث يتم إنشاء المقابس المستندة إلى الملفات.

اعتماداً على كيفية الاتصال، يتم مصادقة العملاء بطرق مختلفة. يحدد ملف التكوين **pg_hba.conf** من الذي يسمح له بالاتصال على كل مقبس وكيفية مصادقته. بشكل افتراضي، تستخدم الاتصالات على مأخذ التوصيل المستند إلى الملفات حساب مستخدم Unix كاسم مستخدم PosgreSQL، ويفترض أنه لا توجد مصادقة أخرى مطلوبة. في اتصال TCP، يطلب PostgreSQL من المستخدم المصادقة باستخدام اسم مستخدم وكلمة مرور (على الرغم من أنه ليس اسم مستخدم/كلمة مرور Unix ولكن بدلاً من ذلك واحد يديره PostgreSQL نفسه).

مستخدم **postgres** خاص ولديه امتيازات إدارية كاملة على جميع قواعد البيانات. سنستخدم هذه الهوية لإنشاء مستخدمين جدد وقواعد بيانات جديدة.

٢.٣.٣.٥. إنشاء المستخدمين وقواعد البيانات

يضيف الأمر **createuser** مستخدمًا جديدًا ويزيل **dropuser** المستخدم. وبالمثل، يضيف الأمر **createdb** قاعدة بيانات جديدة ويزيل **dropdb** قاعدة بيانات. كل من هذه الأوامر لها صفحات يدوية خاصة بها ولكننا سنناقش بعض الخيارات هنا. يعمل كل أمر على الكتلة " cluster" الافتراضية (يعمل على المنفذ 5432) ولكن يمكنك تمرير:

--port=*port*

لتعديل المستخدمين وقواعد البيانات الخاصة بالكتلة البديلة.

يجب أن تتصل هذه الأوامر بخادم PostgreSQL للقيام بعملهم ويجب أن تتم مصادقتهم كمستخدم يتمتع بامتيازات كافية ليتمكنوا من تنفيذ العملية المحددة. أسهل طريقة لتحقيق ذلك هي استخدام حساب Unix **postgres** والاتصال عبر المقبس المستند إلى الملفات " file-based socket":

```
# su - postgres
$ createuser -P king_phisher
Enter password for new role:
Enter it again:
$ createdb -T template0 -E UTF-8 -O king_phisher king_phisher
$ exit
```

في المثال السابق، يطلب الخيار **P-** من الأمر **createuser** تعيين كلمة مرور جديدة لحساب **king_phisher** بمجرد إنشائه. بالنظر إلى الأمر **createdb**، يحدد الخيار **O-** المستخدم الذي يمتلك قاعدة البيانات الجديدة (الذي يتمتع بالتالي بحقوق كاملة لإنشاء الجداول ومنح الأذونات وما إلى ذلك). نريد أيضًا أن نكون قادرين على استخدام سلاسل Unicode، لذلك نضيف الخيار **E UTF-8-** لضبط الترميز، والذي بدوره يتطلب منا استخدام خيار **T-** لاختيار قالب قاعدة بيانات آخر.

يمكننا الآن اختبار إمكانية الاتصال بقاعدة البيانات عبر الاستماع إلى مأخذ التوصيل على المضيف المحلي (**-h localhost**) كمستخدم king_phisher (**-U king_phisher**):

```
# psql -h localhost -U king_phisher king_phisher
Password for user king_phisher:
psql (9.5.2)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help. king_phisher=>
```

كما ترى، نجح الاتصال.

٣.٣.٣.٥. إدارة مجموعات PostgreSQL

أولاً، تجدر الإشارة إلى أن مفهوم "مجموعة -cluster– PostgreSQL" هو إضافة خاصة بـ Debian ولن تجد أي إشارة لهذا المصطلح في وثائق PostgreSQL الرسمية. من وجهة نظر أدوات PostgreSQL، فإن هذه المجموعة هي مجرد مثيل لخادم قاعدة بيانات يعمل على منفذ معين.

ومع ذلك، توفر حزمة ديبيان postgresql الشائعة أدوات متعددة لإدارة هذه المجموعات:

pg_createcluster, **pg_dropcluster**, **pg_ctlcluster**, **pg_upgradecluster**, **pg_renamecluster**, **pg_lsclusters.**

لن نغطي جميع هذه الأدوات هنا، ولكن يمكنك الرجوع إلى الصفحات اليدوية الخاصة بها لمزيد من المعلومات.

ما يجب أن تعرفه هو أنه عندما يتم تثبيت إصدار رئيسي جديد من PostgreSQL على نظامك، فإنه سيقوم بإنشاء مجموعة جديدة تعمل على المنفذ التالي (عادة 5433) وستستمر في استخدام الإصدار القديم حتى تقوم بترحيل قواعد البيانات الخاصة بك من المجموعة القديمة إلى الجديدة.

يمكنك استرداد قائمة بجميع المجموعات وحالتها باستخدام أمر: **pg_lsclusters**. الأهم من ذلك، يمكنك أتمتة ترحيل نظامك إلى أحدث إصدار من PostgreSQL باستخدام:

```
pg_upgradecluster old-version cluster-name
```

لكي ينجح هذا، قد تحتاج أولاً إلى إزالة نظام المجموعة (empty) الذي تم إنشاؤه من أجل الإصدار الجديد (باستخدام: **pg_dropcluster** *new-version cluster-name*). لا يتم إسقاط المجموعة القديمة في العملية، ولكن لن يتم بدء تشغيلها تلقائيًا أيضًا. يمكنك إسقاطها بمجرد التحقق من أن المجموعة التي تمت ترقيتها تعمل بشكل جيد.

٤.٣.٥. تكوين أباتشي

يشتمل التثبيت النموذجي لـ Kali Linux على خادم الويب Apache، الذي توفره حزمة apache2. كونها خدمة شبكة، يتم تعطيلها بشكل افتراضي. يمكنك تشغيله يدويًا باستخدام:

systemctl start apache2.

مع انتشار الكثير والكثير من تطبيقات الويب صار من المهم أن يكون لديك بعض المعرفة بـ Apache من أجل استضافة هذه التطبيقات، سواء للاستخدام المحلي أو لإتاحتها عبر الشبكة.

Apache هو خادم وحدات -modular server- ويتم تنفيذ العديد من الميزات بواسطة وحدات -modules- خارجية يقوم البرنامج الرئيسي بتحميلها أثناء التهيئة. يتيح التكوين الافتراضي فقط الوحدات -modules- الأكثر شيوعًا، ولكن تمكين الوحدات الجديدة يتم بسهولة عن طريق تشغيل **a2enmod** *module*. استخدم **a2dismod** *module* لتعطيل الوحدة. تقوم هذه البرامج في الواقع بإنشاء (أو حذف) روابط رمزية فقط في:

||**a2enmod** "**a**pache **2** **en**able **mod**ule".

a2dismod "**a**pache **2** **dis**able **mod**ule"||

/etc/apache2/mods-enabled/

مشيرة إلى الملفات الحقيقية (المخزنة في **/etc/apache2/mods-available/**).

هناك العديد من الوحدات المتاحة، ولكن هناك اثنتان تستحق النظر الأولي: PHP وSSL. يتم تنفيذ تطبيقات الويب المكتوبة باستخدام PHP بواسطة خادم الويب Apache بمساعدة الوحدة المخصصة التي توفرها حزمة libapache-mod-php، وعند تثبيتها تمكن الوحدة تلقائيا.

يتضمن Apache 2.4 وحدة SSL المطلوبة لـ HTTP الآمن (HTTPS) خارج الصندوق. يجب أولاً تمكينه باستخدام: **a2enmod ssl**، ثم يجب إضافة التوجيهات المطلوبة لملفات التكوين. يتوفر مثال التكوين في **/etc/apache2/sites-available/default-ssl.conf**. راجع http://httpd.apache.org/docs/2.4/mod/mod_ssl.html لمزيد من المعلومات.

يمكن العثور على القائمة الكاملة لوحدات Apache القياسية عبر الإنترنت في http://httpd.apache.org/docs/2.4/mod/index.html.

باستخدام التكوين الافتراضي، يستمع خادم الويب على المنفذ 80 (كما تم تكوينه في **/etc/apache2/ports.conf**)، وصفحات الخادم من المجلد **/var/www/html/** بشكل افتراضي (كما تم تكوينه في **/etc/apache2/sites-enabled/000-default.conf**).

١.٤.٣.٥. تكوين المضيفين الافتراضيين

المضيف الافتراضي هو هوية إضافية لخادم الويب. يمكن أن تخدم عملية أباتشي نفسها مواقع ويب متعددة (مثل www.kali.org و www.offensive-security.com) لأن طلبات HTTP تتضمن كلاً من اسم موقع الويب المطلوب وعنوان URL المحلي (تُعرف هذه الميزة باسم: *namebased virtual hosts*).

يتيح التكوين الافتراضي لـ Apache 2 تمكين name-based virtual hosts. بالإضافة إلى ذلك، يتم تعريف مضيف افتراضي افتراضيا في ملف **/etc/apache2/sites-enabled/000-default.conf**؛ سيتم استخدام هذا المضيف الافتراضي إذا لم يتم العثور على مضيف مطابق للطلب الذي أرسله العميل.

مهم

سيتم دائمًا تقديم الطلبات المتعلقة بالمضيفات الافتراضية غير المعروفة بواسطة المضيف الافتراضي المحدد أولا، ولهذا السبب تقوم الحزمة بشحن ملف تكوين **000-default.conf**، والذي يتم فرزه أولاً بين جميع الملفات الأخرى التي قد تقوم بإنشائها.

يتم بعد ذلك وصف كل مضيف افتراضي إضافي بواسطة ملف مخزن في **/etc/apache2/sites-available/**. عادةً ما تتم تسمية الملف باسم موقع الويب متبوعًا بامتداد **conf**. (على سبيل المثال: **www.example.com.conf**). يمكنك بعد ذلك تمكين المضيف الافتراضي الجديد باستخدام: *www.example.com* **a2ensite**. فيما يلي الحد الأدنى من تكوين المستضيف الافتراضي لموقع ويب يتم تخزين ملفاته في **/srv/www.example.com/www/** (محدد بخيار **DocumentRoot**):

```
ServerName www.example.com
ServerAlias example.com
DocumentRoot /srv/www.example.com/www
```

قد تفكر أيضًا في إضافة توجيهات `CustomLog` و `ErrorLog` لتكوين Apache لإخراج سجلات الدخول في ملفات مخصصة للمضيف الافتراضي.

٢.٤.٣.٥. توجيهات شائعة الإستخدام

يستعرض هذا القسم بعض توجيهات تكوين Apache شائعة الاستخدام.

عادة ما يتضمن ملف التكوين الرئيسي العديد من كتل **Directory** -مجلد-، أنها تسمح بتحديد سلوكيات مختلفة للخادم حسب موقع الملف الذي يتم تقديمه. تتضمن مثل هذه الكتلة الشائعة **Options** و **AllowOverride**:

```
Options Includes FollowSymLinks
AllowOverride All
DirectoryIndex index.php index.html index.htm
```

يحتوي التوجيه **DirectoryIndex** على قائمة بالملفات التي يجب تجربتها عندما يطابق طلب العميل مجلدا. يتم استخدام أول ملف موجود في القائمة وإرساله كرد.

ويتبع توجيه **Options** قائمة من الخيارات للتمكين. تقوم القيمة **None** بتعطيل جميع الخيارات، وبالمثل، فإن **All** يمكّنهم جميعًا باستثناء **MultiViews**. تشمل الخيارات المتاحة:

- ❖ **ExecCGI** - يشير إلى أنه يمكن تنفيذ البرامج النصية CGI.
- ❖ **FollowSymLinks** - تخبر الخادم أنه يمكنه اتباع الروابط الرمزية، وأن الاستجابة يجب أن تحتوي على محتويات هدف هذه الروابط.

- **SymLinksIfOwnerMatch** - يخبر الخادم أيضًا باتباع الروابط الرمزية، ولكن فقط عندما يكون للرابط وهدفه المالك نفسه.
- **Includes**- يمكّن تضمين جانب الخادم -*Server Side Includes*- (SSI). هذه توجيهات مضمنة في صفحات HTML وتنفيذها على الفور لكل طلب.
- **Indexes**– تطلب من الخادم إدراج محتويات المجلد إذا كان طلب HTTP الذي أرسله العميل يشير إلى مجلد بدون ملف فهرس (أي عندما لا توجد ملفات مذكورة في توجيه **DirectoryIndex** في هذا المجلد).
- **MultiViews** - تتيح التفاوض -negotiation- على المحتوى؛ يمكن استخدام هذا من قبل الخادم لإرجاع صفحة ويب مطابقة للغة المفضلة كما تم تكوينه في المستعرض.

٥.٣.٤.٢.١. طلب المصادقة

في بعض الحالات، يجب تقييد الوصول إلى جزء من موقع ويب، لذلك يتم منح حق الوصول إلى المحتويات للمستخدمين الشرعيين فقط الذين يقدمون اسم مستخدم وكلمة مرور.

يحتوي ملف **htaccess.** على توجيهات تكوين Apache التي يتم فرضها في كل مرة يتعلق فيها الطلب بعنصر من المجلد حيث يتم تخزين ملف **htaccess.**. هذه التوجيهات متكررة، مما يوسع النطاق ليشمل جميع المجلدات الفرعية.

معظم التوجيهات التي يمكن أن تحدث في كتلة **Directory** قانونية أيضًا في ملف **htaccess.**. يسرد الأمر **AllowOverride** جميع الخيارات التي يمكن تمكينها أو تعطيلها عن طريق **htaccess.**. الاستخدام الشائع لهذا الخيار هو تقييد **ExecCGI**، بحيث يختار المسؤول المستخدمين المسموح لهم بتشغيل البرامج تحت هوية خادم الويب (مستخدم الـ **www-data**).

مثال ٣.٥. **htaccess.** ملف يتطلب المصادقة

```
Require valid-user
AuthName "Private directory"
AuthType Basic
AuthUserFile /etc/apache2/authfiles/htpasswd-private
```

لا توفر المصادقة الأساسية -Basic- الأمان

يتمتع نظام المصادقة المستخدم في المثال السابق (`Basic`) بالحد الأدنى من الأمان حيث يتم إرسال كلمة المرور بنص واضح (يتم ترميزها فقط كـ *base64*، وهو ترميز بسيط بدلاً من أسلوب تشفير). وتجدر الإشارة أيضًا إلى أن المستندات التي تحميها هذه الآلية أيضًا تمر عبر الشبكة بشكل واضح. إذا كان الأمان مهمًا، فيجب تشفير جلسة HTTP بالكامل باستخدام طبقة النقل الآمنة (TLS).

يحتوي الملف **/etc/apache2/authfiles/htpasswd-private** على قائمة بالمستخدمين وكلمات المرور، يتم التلاعب بها عادة باستخدام الأمر **htpasswd**. على سبيل المثال، يتم استخدام الأمر التالي لإضافة مستخدم أو تغيير كلمة المرور الخاصة به:

```
# htpasswd /etc/apache2/authfiles/htpasswd-private user
New password: Re-type new password: Adding password for user user
```

٢.٢.٤.٣.٥. تقييد الوصول

يتحكم التوجيه **Require** في قيود الوصول إلى المجلد (والمجلدات الفرعية الخاصة به، بشكل متكرر).

يمكن استخدامه لتقييد الوصول على أساس العديد من المعايير، سنتوقف عند وصف تقييد الوصول استنادًا إلى عنوان IP للعميل ولكن يمكن جعله أكثر قوة من ذلك، خاصة عندما يتم دمج العديد من التوجيهات المطلوبة -**Require**- داخل كتلة **RequireAll**،

على سبيل المثال، يمكنك تقييد الوصول إلى الشبكة المحلية باستخدام التوجيه التالي:

```
Require ip 192.168.0.0/16
```

4.5. إدارة الخوادم

يستخدم كالي **systemd** كنظام خاص به، وهو ليس مسؤولًا فقط عن تسلسل الإقلاع، ولكنه يعمل أيضًا بشكل دائم كمدير خوادم كامل الميزات لبدء ومراقبة الخدمات.

يمكن الاستعلام عن **systemd** والتحكم فيه باستخدام **systemctl**. بدون أي مدخلات، يقوم بتشغيل الأمر **systemctl list-units** الذي ينتج قائمة *بالوحدات* النشطة. إذا قمت بتشغيل **systemctl status**، يعرض الإخراج نظرة عامة هرمية للخدمات قيد التشغيل. بمقارنة كل من المخرجات، ترى على الفور أن هناك أنواعًا متعددة من الوحدات وأن الخدمات واحدة فقط بينها.

يتم تمثيل كل خدمة *بوحدة خدمة -service unit-*، والتي يتم وصفها بملف خدمة يتم شحنها عادةً في **/lib/systemd/system/** (أو **/run/systemd/system/**، أو **/etc/systemd/system/** ؛ يتم إدراجها عن طريق زيادة ترتيب الأهمية، وآخر واحد يفوز). ربما يتم تعديل كل منها عن طريق ملفات *service-name*.**service.d/*.conf** أخرى في نفس مجموعة المجلدات. ملفات الوحدات هذه هي ملفات نصية عادية تعرف بامتداد "*.ini" أحيانا المعروفة في Microsoft Windows، مع أزواج *key = value* مجمعة بين رؤوس [*section*]. نرى هنا ملف خادم بسيط لـ **/lib/systemd/system/ssh.service**:

```
[Unit]
Description=OpenBSD Secure Shell server
After=network.target auditd.service
```

```
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
Type=notify

[Install]
WantedBy=multi-user.target
Alias=sshd.service
```

الوحدات المستهدفة هي جزء آخر من تصميم النظام. تمثل الحالة المرغوبة التي تريد تحقيقها من حيث الوحدات النشطة (مما يعني خدمة جارية في حالة وحدات الخدمة). وهي موجودة بشكل أساسي كوسيلة لتجميع التبعيات على الوحدات الأخرى. عندما يبدأ النظام، فإنه يمكّن الوحدات المطلوبة للوصول إلى **default.target** (وهي وصلة رمزية لـ **graphical.target** والذي يعتمد بدوره على **multi-user.target**). لذلك يتم تنشيط جميع تبعيات تلك الأهداف أثناء الإقلاع.

يتم التعبير عن هذه التبعيات بتوجيه **Wants** على الوحدة المستهدفة. ولكن ليس عليك تعديل الوحدة المستهدفة لإضافة تبعيات جديدة، يمكنك أيضًا إنشاء وصلة رمزية تشير للوحدة التابعة في المجلد **/etc/systemd/system/***target-name***.target.wants/**.

وهذا بالضبط ما يفعله *foo.service* **systemctl enable**. عندما تقوم بتمكين خدمة، فأنت تخبر systemd أن يضيف تبعية على الأهداف المدرجة في إدخال **WantedBy** لقسم [**install**] لملف وحدة الخدمة. عكس ذلك، يقوم **systemctl** *foo.service* **disable** بتعطيل نفس الوصلة الرمزية وبالتالي التبعية.

أمرا **enable** و **disable** لا تغير أي شيء يتعلق بالحالة الحالية للخدمات. إنهم تؤثران فقط على ما سيحدث في الإقلاع التالي. إذا كنت ترغب في تشغيل الخدمة على الفور، فيجب عليك تشغيل: *foo.service* **systemctl start**. على العكس من ذلك، يمكنك إيقافه من خلال *foo.service* **systemctl stop**. يمكنك أيضًا فحص الحالة الحالية للخدمة باستخدام: *foo.service* **systemctl status**، والتي تتضمن بشكل مفيد أحدث أسطر من السجل المرتبط. بعد تغيير تكوين الخدمة، قد ترغب في إعادة تحميلها أو إعادة تشغيلها: تتم هذه العمليات باستخدام: **systemctl** *foo.service* **reload** و *foo.service* **systemctl restart** على التوالي.

systemctl status postgresql

● postgresql.service - PostgreSQL RDBMS

Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)

Active: inactive (dead)

ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service

ls: cannot access '/etc/systemd/system/multi-user.target.wants/postgresql.service': No such file or directory

```
# systemctl enable postgresql
[...]
# ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service
lrwxrwxrwx 1 root root 38 Apr 21 16:21 /etc/systemd/system/multi-user.target.wants/postgresql.service -> /lib/systemd/system/postgresql.service

# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
# systemctl start postgresql
# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: disabled)
   Active: active (exited) since Thu 2016-04-21 16:22:29 EDT; 2s ago
  Process: 6355 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 6355 (code=exited, status=0/SUCCESS)

Apr 21 16:22:29 kali-rolling systemd[1]: Starting PostgreSQL RDBMS...
Apr 21 16:22:29 kali-rolling systemd[1]: Started PostgreSQL RDBMS.
```

٥.٥. الملخص

تعلمنا في هذا الفصل كيفية تكوين Kali Linux. قمنا بتكوين إعدادات الشبكة، وتحدثنا عن المستخدمين والمجموعات، وناقشنا كيفية إنشاء وتعديل حسابات المستخدمين، وتعيين كلمات المرور، وتعطيل الحسابات، وإدارة المجموعات. أخيرًا، ناقشنا الخدمات وشرحنا كيفية إعداد الخدمات العامة وصيانتها، وتحديدًا SSH و PostgreSQL و Apache.

نصائح الملخص:

❖ في التثبيت النموذجي لسطح المكتب، سيكون لديك NetworkManager مثبتًا بالفعل ويمكن التحكم فيه وتكوينه من خلال مركز التحكم في GNOME ومن خلال القائمة العلوية اليمنى.

❖ يمكنك تكوين الشبكة من خلال سطر الأوامر باستخدام أدوات **ifup** و **ifdown**، التي تقرأ تعليماتها من ملف التكوين **/etc/network/interfaces**. أداة أحدث، *systemd-networkd* تعمل مع نظام *systemd* init.

❖ بشكل افتراضي، تتكون قاعدة بيانات مستخدمي ومجموعات Unix من ملفات نصية **/etc/passwd** (قائمة المستخدمين)، **/etc/shadow** (كلمات المرور المشفرة للمستخدمين)، **/etc/group** (قائمة المجموعات)، و **/etc/gshadow** (كلمات المرور المشفرة للمجموعات).

❖ يمكنك استخدام الأمر **getent** لاستشارة قاعدة بيانات المستخدم وقواعد بيانات النظام الأخرى.

❖ يطرح أمر **adduser** بعض الأسئلة قبل إنشاء الحساب، ولكنها الطريقة المباشرة لإنشاء حساب مستخدم جديد.

❖ يمكن استخدام عدة أوامر لتعديل حقول معينة في قاعدة بيانات المستخدم بما في ذلك: **passwd** (تغيير كلمة المرور)، **chfn** (تغيير الاسم الكامل و**GECOS**، أو حقل المعلومات العامة)، **chsh** (تغيير تسجيل الدخول الصدفة)، **chage** (تغيير عمر كلمة المرور)،و **passwd -e** *user* (يجبر المستخدم على تغيير كلمة المرور الخاصة به في المرة التالية التي يقوم فيها بتسجيل الدخول).

❖ يمكن لكل مستخدم أن يكون عضوا في مجموعة واحدة أو مجموعات متعددة. يمكن استخدام عدة أوامر لتعديل هوية المجموعة: يغير **newgrp** معرف المجموعة الحالي، **sg** ينفذ أمرًا باستخدام المجموعة البديلة المزودة، ويمكن وضع بت **setgid** في مجلد، مما يؤدي إلى أن تنتمي الملفات التي تم إنشاؤها في هذا المجلد تلقائيًا إلى المجموعة الصحيحة. بالإضافة إلى ذلك، يعرض الأمر **id** الحالة الحالية للمستخدم بما في ذلك قائمة بعضوية مجموعته.

❖ يمكنك بدء SSH يدويًا باستخدام **systemctl start ssh** أو تمكينه بشكل دائم باستخدام **systemctl enable ssh**. يعطل التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى كلمة المرور للمستخدم الجذر، مما يعني أنه يجب عليك أولاً إعداد مفاتيح SSH باستخدام **ssh-keygen**.

❖ PostgreSQL هو خادم قاعدة بيانات. نادرًا ما يكون مفيدًا من تلقاء نفسه ولكن يتم استخدامه من قبل العديد من الخدمات الأخرى لتخزين البيانات.

❖ يشتمل التثبيت النموذجي لـ Kali Linux على خادم الويب Apache، الذي توفره حزمة apache2. كونها خدمة شبكة، يتم تعطيلها بشكل افتراضي. يمكنك تشغيله يدويًا باستخدام **systemctl start apache2**.

❖ من خلال التكوين الافتراضي، يستمع Apache على المنفذ 80 (كما تم تكوينه في **/etc/apache2/ports.conf**)، ويقدم صفحات من المجلد **/var/www/html/** افتراضيًا (كما تم تكوينه في **/etc/apache2/sites-enabled/000-default.conf**).

الآن بعد أن تعاملنا مع أساسيات Linux وتثبيت Kali Linux وتكوينه، دعنا نناقش كيفية تحرّي الخلل وإصلاحه وتعليمك بعض الأدوات والحيل لإعادتك للعمل عند مواجهة المشاكل.

التمرين الأول، الفصل الخامس - تكوين المستخدمين

١. قم بإنشاء حساب مستخدم قياسي. أضف المستخدم الجديد إلى مجموعة "sudo"

الإجابة:

```
adduser username
passwd username
usermod -a -G sudo username
chsh -s /bin/bash username
```

التمرين الثاني، للفصل الخامس - تكوين الشبكة

٢. أوقف خدمة Network Manager وقم بتعطيلها بالكامل في وقت الإقلاع.

٣. تكوين جهاز Kali الخاص بك لـ DHCP على eth0

٤. إنزال واجهة eth0.

٥. اتصل بالشبكة اللاسلكية باستخدام دونجل USB اللاسلكي الخاص بك عن طريق تكوين /etc/network/interfaces وفقًا لذلك.

الإجابة:

١. مدير الشبكة مفيد، ولكن في اختبار الإختراق تحتاج حقًا إلى الاستيلاء على واجهاتك وثنيها حسب إرادتك دون أي مفاجآت. لإيقاف Network Manager وتعطيله في وقت الإقلاع:

```
systemctl stop NetworkManager.service
systemctl disable NetworkManager.service
```

يمكنك التحقق من حالة الواجهات المُدارة في Network Manager من خلال:

```
nmcli dev status
```

نصيحة احترافية: أوقف مدير الشبكة من خلال إضافة dns-servers إلى ملف /etc/resolv.conf:

```
nano /etc/NetworkManager/NetworkManager.conf
```

أضف dns=none لقسم [main].

٢. اضبط eth0 لـ DHCP. قم بتغير ملف /etc/network/interfaces لتضمين:

```
auto eth0
iface eth0 inet dhcp
```

يمكنك أيضًا إعداد عنوان ثابت باستخدام ما يلي:

```
auto eth0

iface eth0 inet static

      address 192.168.1.160

      netmask 255.255.255.0

      gateway 192.168.1.1
```

٣. إنزال واجهة eth0:

ifconfig eth0 down

٤. الاتصال بشبكة لاسلكية. لاحظ أنه إذا كنت في جهاز إفتراضي، فستحتاج إلى محول لاسلكي USB. يفترض هذا المثال WPA2.Generate psk باستخدام الأمر التالي:

wpa_passphrase myssid wpa-password

الآن قم بإدراج PSK مع ما يلي داخل ملف /etc/network/interfaces:

```
auto wlan0

iface wlan0 inet dhcp

    wpa-ssid myssid

    wpa-psk {whatever the psk hash was}
```

قم بتدوير الواجهة:

ifup wlan0

التمرين الثالث، للفصل الخامس - تكوين الخدمات الجزء ١

١. تكوين SSH للسماح بتسجيل الدخول الجذر باستخدام كلمة المرور (تلميح: PermitrootLogin).
٢. ابدأ تشغيل خدمة SSH واتصل بها من النظام المضيف كمستخدم root.
٣. تكوين خدمة SSH للبدء في وقت الإقلاع.
٤. قم بتغيير كلمة مرور الجذر وقم بإنشاء مفاتيح مضيف SSH جديدة.
٥. النينجا! اجعل نسخة Kali الخاصة بك نقطة وصول عن طريق تثبيت **hostapd** وبدء تشغيله في وقت الإقلاع. قم بذلك بتكوين خدمة نظام مخصص! *هذا الجزء من التمرين قيد الاختبار.*

الإجابة:

١. عين **PermitrootLogin** لـ **yes** في /etc/ssh/sshd_config

٢. ابدء sshd:

systemctl start ssh

٣. تمكين sshd عند الإقلاع:

systemctl enable ssh

٤. لأسباب أمنية، قم بتغيير كلمة مرور الجذر وقم بإنشاء مفاتيح مضيف SSH جديدة:

```
root@kali:~# passwd
[...]
root@kali:~# rm /etc/ssh/ssh_host_*
root@kali:~# dpkg-reconfigure openssh-server
root@kali:~# service ssh restart
```

٥. النينجا فقط! hostapd (برنامج نقطة الوصول للمضيف) هو نقطة وصول لبرامج مساحة المستخدم قادرة على تحويل بطاقات واجهة الشبكة العادية إلى نقاط وصول وخوادم مصادقة. لتهيئة خدمة hostapd يدويًا من خلال systemd:

تثبيت وتكوين المتطلبات الأساسية:

```
apt-get install hostapd
nano /etc/systemd/system/hostapd.service
```

أضف الاختبار التالي لملف hostapd.service:

```
[Unit]

Description=Hostapd WPE Service

After=network.target


[Service]

Type=simple

User=root

ExecStart=/usr/sbin/hostapd /etc/hostapd/hostapd.conf

Restart=on-abort


[Install]

WantedBy=multi-user.target
```

- قم بإنشاء أو نسخ ملف hostapd.conf إلى /etc/hostapd/hostapd.conf
- تعطيل مدير الشبكة! أعد تشغيل الخدمة وتمكينها في وقت الإقلاع. تأكد من أن hostapd يعمل بالفعل عند بدء الخدمة.

```
systemctl stop NetworkManager.service
systemctl disable NetworkManager.service
sudo nmcli radio wifi off
sudo rfkill unblock wlan
systemctl enable hostapd
systemctl start hostapd
ps -ef |grep hostapd
systemctl status hostapd
systemctl stop hostapd
ps -ef |grep hostapd
```

ملاحظة: إذا كنت تعمل على جهاز افتراضي، أو كنت تستخدم بطاقة Atheros، فقد تواجه مشكلات ("EEPROM magic" أو فشل البرامج الثابتة، وما إلى ذلك) مع المحول اللاسلكي المستند إلى USB. إذا كانت هذه هي الحالة، أخرج "eject" المحول في إعدادات VM الخاصة بك، افصله، أغلق VM بشكل سليم. أدخل البطاقة وقم بتشغيل الجهاز الافتراضي. إذا لم ينجح أي من هذا، فلا تقلق. هذا أمر صعب للغاية خاصة بسبب VM.

ملاحظة: **systemctl status hostapd** هو pal استكشاف الأخطاء وإصلاحها.

التمرين الرابع، الفصل الخامس - تكوين الخدمات الجزء الثاني

في هذا التمرين، سنقوم بتثبيت masscan. هذه أداة رائعة وسيساعد التثبيت الكامل في مراجعة بعض مفاهيم التكوين التي استكشفناها في هذا الفصل. يتم تقسيم العملية إلى عدة خطوات:

١. قم بتثبيت واباتشي خدمات PostgreSQL.
٢. كوِّن أباتشي و PostgreSQL للبدء في وقت الإقلاع.
٣. قم بتثبيت masscan، وهي متطلبات مسبقة وواجهة ويب ماسكان للأمن الشامل. استخدم حزم Apache / PostgreSQL.

Install masscan, it's prerequisites and Offensive Security's masscan web interface. Use an Apache / PostgreSQL stack.

٤. استيراد فحص سابق واعرض النتائج.
٥. قم بحماية تثبيت Apache باستخدام htaccess اسم مستخدم / كلمة مرور.

الإجابات:

سيكون هذا الحل معطلاً قليلاً. للبدء، راجع نسخة من مستودع masscan-web-ui:

```
root@kali:~# cd /root/
root@kali:~# git clone https://github.com/offensive-security/masscan-web-ui
```

بعد ذلك، تأكد من وجود جميع متطلبات masscan الرئيسية ونسخها عبر ملفات واجهة الويب MASSCAN إلى جذر الويب. لاحظ أنه إذا كنت تقوم بنسخ ولصق سطر **apt-get**، فهذا طويل. تأكد من انتزاع كل شيء:

```
root@kali:~# apt-get install apache2 php libapache2-mod-php php-xml postgresql php-pgsql
mv masscan-web-ui/* /var/www/html/
rm /var/www/html/index.html
```

إبدء تشغيل Apache و Postgres:

```
systemctl start apache2
systemctl start postgresql
```

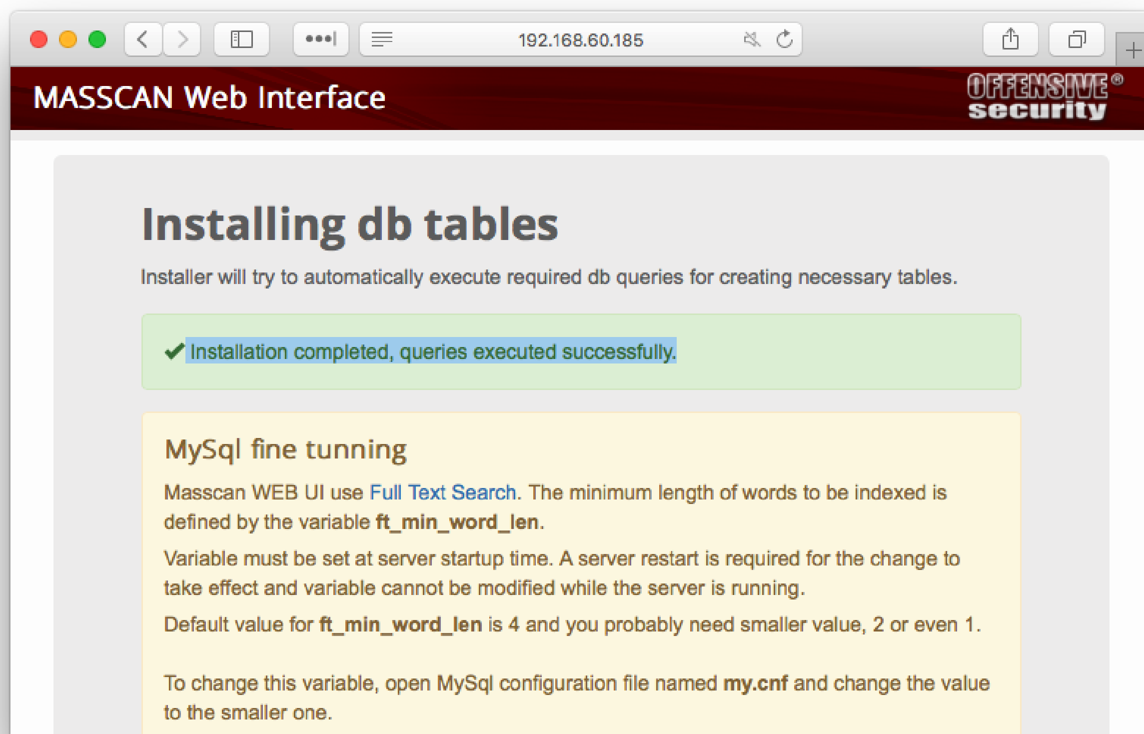
مع بدء Apache و PostgreSQL، تثبيت masscan و index.html الافتراضي من Apache، يمكنك تصفح خادم Apache الخاص بك لرؤية ماسكان. ومع ذلك، فإنه يشكو بحق من فشل مصادقة كلمة المرور. دعنا نصلح ذلك. إنشاء مستخدم ماسكان وإنشاء قاعدة بيانات ماسكان.

```
root@kali:~# su - postgres
postgres@kali:~$ createuser -P masscan
Enter password for new role:
Enter it again:
postgres@kali:~$ createdb -T template0 -E UTF-8 -O
masscan masscandb
exit
```

بعد ذلك، قم بتعديل كلمة المرور التي قمت بتعيينها واسم قاعدة البيانات (masscandb) في أسطر **define**:

```
root@kali:~# nano /var/www/html/config.php
[...]
root@kali:~# grep ^define /var/www/html/config.php
define('DB_DRIVER',        'pgsql');
define('DB_HOST',       '127.0.0.1');
define('DB_USERNAME',  'masscan');
define('DB_PASSWORD',  'toortoor');
define('DB_DATABASE',  'masscandb');
```

تصفح http://localhost على جهازك المحلي (أو العنوان البعيد إذا كنت تتصفح من خارج الجهاز الإفتراضي) والذي يجب أن يشير إلى أنه تم إعداد ماسكان بشكل صحيح:



بعد ذلك، دعنا نستورد بعض نتائج الفحص من فحص تم تشغيله مسبقًا. سنقوم بمسح قاعدة البيانات لأن هذه هي المرة الأولى التي نستخدم فيها ماسكان:

```
root@kali:~# wget https://kali.training/downloads/masscan.xml
root@kali:~# php /var/www/html/import.php /root/masscan.xml
Do you want to clear the database before importing (yes/no)?: yes

Clearing the db
Reading file
Parsing file
```

```
Processing data (This may take some time depending on file size)

Summary:
Total records:4646
Inserted records:4646
Took about:10 seconds
root@kali:~#
```

بعد ذلك، تصفح http://localhost لعرض البيانات المستوردة. نظرًا لأن هذه "بيانات حساسة"، فإننا نريد حماية مجلد الويب الجذر بكلمة مرور. للقيام بذلك، يجب أن نبدأ بتوجيهات Apache:

```
root@kali:~# nano /etc/apache2/sites-enabled/000-default.conf
```

أضف هذه الأسطر:

```
AuthType Basic
AuthName "Restricted Content"
AuthUserFile /etc/apache2/htpasswd
Require valid-user
```

ودعنا ننشئ بيانات اعتماد لمستخدم جديد:

```
root@kali:~# htpasswd -c /etc/apache2/htpasswd myuser
```

أخيرًا، استعرض تصفح http://localhost، وأدخل بيانات اعتمادك واعرض التقرير.

هل تعلم؟

هل تتذكر سياسة Kali Linux لتعطيل خدمات الشبكة افتراضياً؟ تم تكوين هذه السياسة من

/lib/systemd/system-preset/{95-kali.preset،99-default.preset}

نقطة وصول راسبيري باي

إذا لم يكن لديك Raspberry Pi 3، فعليك الحصول على واحدة. فهي رائعة للغاية وغير مكلفة نسبيًا. في هذا التمرين، ستقوم بتكوين Raspberry Pi 3 ليتم تشغيله كنقطة وصول لاسلكية، مما يمنح المستخدمين المتصلين إمكانية الوصول إلى الإنترنت. هذا التمرين رائع لأنك ستقوم بتثبيت Kali على Raspberry Pi وتعديل الملفات وتغيير أذونات الملفات وتكوين واجهات الشبكة وتثبيت الخدمات وتكوينها وتكوين قواعد iptables والمزيد. إنها نظرة عامة رائعة.

إليك ما عليك القيام به:

١. قم بتثبيت Kali على Raspberry Pi 3. يمكنك استخدام صورة مخصصة، ولكن إذا قمت بذلك، فقد يكون لديك المزيد من استكشاف الأخطاء وإصلاحها. إذا لم تكن متأكدًا، فاستخدم صورة المخزون التي تمت كتابة هذا الحل من أجلها.

٢. تطبيق أمان WPA2 على AP.

٣. قم بتكوين **eth0** على أنه DHCP، و**wlan0** على أنه ثابت.

٤. قم بتكوين Raspberry Pi كخادم DHCP لأي عميل لاسلكي وتعيين مصادقة بـ DHCP لمدة ١٢ ساعة.

٥. اجعل خادم SSH يبدأ في وقت الإقلاع حتى تمكن SSH إلى Raspberry Pi بمجرد تشغيله.

٦. إعادة توجيه كل حركة المرور الصادرة، بما في ذلك DNS، من **wlan0** إلى **eth0**.

٧. السماح بالاتصالات الداخلية (ذات الحالة) الواردة من **eth0** إلى **wlan0**.

٨. تلميح: على الرغم من أنك لم نتعلم عن **hostapd** أو **dnsmasq**، إلا أنك ستستخدمها في هذا التمرين.

٩. الغش الجزئي: على الرغم من أن هذا المقال لم يكتب لكالي (ولن يعمل كما هو مكتوب في كالي)، إلا أنه مصدر إلهام لهذا التمرين، ويستحق المراجعة. بفضل فيل مارتن للإلهام.

الإجابات:

سيتطلب هذا بعض الأشياء:

- ❖ Raspberry Pi 3: يمكنك استخدام طراز أقدم بشبكة wifi USB ولكنك لوحدك عندما يتعلق الأمر بتكوين **wlan0**.
- ❖ hostapd: يؤدي هذا إلى إنشاء نقطة اتصال.
- ❖ dnsmasq: يقوم هذا بإعادة توجيه DNS ويوفر قطع DHCP.
- ❖ dhcpcd5: عميل DHCP (الذي يقوم أيضًا بأشياء أخرى رائعة لإدارة الشبكة).

احصل على الحزم المطلوبة:

```
apt-get install dnsmasq hostapd dhcpcd5
```

أولاً، دعنا نطلب من dhcpcd تجاهل إعداد wlan0. سنقوم بتكوين عنوان IP ثابت لاحقًا:

```
nano /etc/dhcpcd.conf
```

ضع هذا فوق أي سطور واجهة قد تكون في الملف:

```
denyinterfaces wlan0
```

الآن، فلنقم بإعداد واجهة wifi الخاصة بنا. إذا كان لديك Pi 2 مع محول USB wi-fi، فتابع وقم بتوصيله الآن. تحرير ملف الواجهات:

```
nano /etc/network/interfaces
```

وأضف هذا القسم:

```
allow-hotplug wlan0

iface wlan0 inet static

    address 172.24.1.1

    netmask 255.255.255.0
```

network 172.24.1.0

broadcast 172.24.1.255

أعد تشغيل dhcpcd باستخدام:

```
root@kali:~# service dhcpcd restart
```

ثم أعد تحميل تكوين wlan0 باستخدام:

```
root@kali:~# ifdown wlan0; ifup wlan0
```

بعد ذلك، فلنقم بتكوين hostapd بملف تكوين جديد. لاحظ أنه تم تكوين SSID وكلمة المرور لنقطة الوصول الخاصة بك.

```
root@kali:~# nano /etc/hostapd/hostapd.conf
[..]
root@kali:~# cat /etc/hostapd/hostapd.conf

# This is the name of the WiFi interface we configured above
interface=wlan0

# Use the nl80211 driver with the brcmfmac driver
driver=nl80211

# This is the name of the network
```

```
ssid=Kali-Pi3

# Use the 2.4GHz band
hw_mode=g

# Use channel 6
channel=6

# Enable 802.11n
ieee80211n=1

# Enable WMM
wmm_enabled=1

# Enable 40MHz channels with 20ns guard interval
ht_capab=[HT40][SHORT-GI-20][DSSS_CCK-40]

# Accept all MAC addresses
macaddr_acl=0

# Use WPA authentication
auth_algs=1

# Require clients to know the network name
ignore_broadcast_ssid=0

# Use WPA2
```

```
wpa=2

# Use a pre-shared key
wpa_key_mgmt=WPA-PSK

# The network passphrase
wpa_passphrase=raspberrytoor

# Use AES, instead of TKIP
rsn_pairwise=CCMP
```

عند هذه النقطة، يمكننا اختبار الأشياء. شغل:

```
root@kali:~# /usr/sbin/hostapd /etc/hostapd/hostapd.conf
```

هذا يدل على تشغيل ناجح. لاحظ أن الأخطاء المتعلقة بوضع المراقبة ليست ذات صلة بنا. بالنسبة إلى RPi3 باستخدام برنامج nexmon، نحتاج (أو تطبيق) ال *nexutil -m2*.

```
root@kali:~# /usr/sbin/hostapd /etc/hostapd/hostapd.conf
Configuration file: /etc/hostapd/hostapd.conf
Failed to create interface mon.wlan0: -95 (Operation not supported)
wlan0: Could not connect to kernel driver
Using interface wlan0 with hwaddr b6:ae:d7:42:a1:70 and ssid "Kali-Pi3"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
```

يمكنك الاتصال بنقطة الوصول هذه وسيعرض hostapd بعض الإخراج:

wlan0: STA 78:4f:43:7c:6d:32 IEEE 802.11: associated

وبمجرد إدخال كلمة المرور، سترى شيئًا مثل هذا:

wlan0: AP-STA-CONNECTED 78:4f:43:7c:6d:32

wlan0: STA 78:4f:43:7c:6d:32 RADIUS: starting accounting session 5991CC2F-00000000

wlan0: STA 78:4f:43:7c:6d:32 WPA: pairwise key handshake completed (RSN)

wlan0: STA 78:4f:43:7c:6d:32 IEEE 802.11: disassociated

wlan0: AP-STA-DISCONNECTED 78:4f:43:7c:6d:32

wlan0: INTERFACE-DISABLED

wlan0: STA 00:00:00:00:00:00 IEEE 802.11: disassociated

wlan0: INTERFACE-ENABLED

wlan0: STA 78:4f:43:7c:6d:32 IEEE 802.11: associated

لاحظ أن عميلك ربما ينقطع الاتصال به ويعاد الاتصال لأنه لم يحصل على عنوان IP. هذا امر طبيعي. لن تحصل على عنوان IP حتى نقوم بتكوين dnsmasq. استمتع بهذا! يمنحك فكرة عن كيفية عمل هذه العملية، خلف الكواليس.

اضغط على Ctrl-C لإيقاف **hostapd**.

بعد ذلك، سنخبر hostapd بمكان العثور على ملف التكوين الخاص به:

```
root@kali:~# nano /etc/default/hostapd
```

ابحث عن سطر ""=DAEMON_CONF# واستبدله بـ:

DAEMON_CONF="/etc/hostapd/hostapd.conf"

لنقم بتعديل **dnsmasq**:

```
root@kali:~# mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
root@kali:~# nano /etc/dnsmasq.conf
```

يجب أن يبدو كالتالي:

```
interface=wlan0       # Use interface wlan0
listen-address=172.24.1.1 # Set our listening address
bind-interfaces      # Bind to the interface to make sure we aren't sending things elsewhere
server=8.8.8.8       # Forward DNS requests to Google DNS
domain-needed        # Don't forward short names
bogus-priv           # Never forward addresses in the non-routed address spaces.
dhcp-range=172.24.1.50,172.24.1.150,12h   # Assign IP addresses between 172.24.1.50 and 172.24.1.150 with a 12 hour lease time
```

الأن لدينا واجهتان نشطتان، وعندنا عميل DHCP لـ الروسفيري الخاص بنا وخادم DHCP لمضيفي الوايرليس الخاص بنا. الأن نحتاج لإعادة توجيه حركة المرور بين واجهات wifi و ethernet. يمكننا تحقيق ذلك على الفور باستخدام أمر بسيط لتحديث proc/:

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
```

ومع ذلك، لن يلتزم هذا التغيير بين عمليات إعادة التشغيل. نحن بحاجة إلى جعلها دائمة من خلال sysctl:

```
root@kali:~# nano /etc/sysctl.conf
```

إلغي تعليق السطر الذي يحتوي على **net.ipv4.ip_forward =1**:

```
root@kali:/var/www/html# grep ip_forward /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

إن عملية إعادة التوجيه ليست كافية تمامًا لمنح مضيفي wifi الخاصين بنا إمكانية الوصول إلى الإنترنت (من خلال واجهة eth0). نحن بحاجة إلى iptables لمساعدتنا على القيام بذلك.

```
root@kali:~# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@kali:~# iptables -A FORWARD -i eth0 -o wlan0 \
> -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
root@kali:~# iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

دعونا نبسط هذه الأوامر:

١. عندما يتم العثور على اتصال جديد (`-t nat`)، نريد تبديل -alter- الحزم لأنها على وشك الخروج (A POSTROUTING-) على واجهة إيثرنت (o eth0-). الهدف -j MASQUERADE يحجب عنوان IP الخاص للعميل بعنوان IP الخارجي لجدار الحماية / البوابة (Kali Pi).

٢. بعد ذلك، نلحق (A-) بقاعدة إلى سلسلة FORWARD (يتم توجيه الحزم عبر Pi) والتي تقبل (j ACCEPT-) الحزم من eth0 إلى wlan0 (i eth0 –o wlan0-) التي تنتمي إلى (ESTABLISHED) أو المتعلقة (RELATED) باتصال موجود.

٣. أخيرًا، سنعيد توجيه -forward - (ونقبل -accept-) جميع الحزم من wlan0 إلى eth0.

تحقق من قواعدنا:

```
root@kali:~# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A  FORWARD  -i  eth0  -o  wlan0  -m  state  --state
RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

إخراج قواعدنا إلى ملف:

```
iptables-save > /etc/iptables.ipv4.nat
```

قم بتطبيق هذه القواعد في كل مرة نقوم فيها بتشغيل Pi عن طريق تحرير ملف **/etc/rc.local**:

```
root@kali:~# nano /etc/rc.local
[...]
root@kali:~# more /etc/rc.local
#!/bin/sh -e
iptables-restore < /etc/iptables.ipv4.nat
```

اجعل الملف قابلاً للتنفيذ:

```
root@kali:~# chmod 711 /etc/rc.local
root@kali:~# ls -l /etc/rc.local
-rwx--x--x 1 root root 57 Aug 10 19:37 /etc/rc.local
```

كما رأينا، يتم شحن **hostapd** و **dnsmasq** مع جميع مزايا نظام التهيئة *-init system-* (انظر /etc/init.d)، لذلك دعونا نبدأ الخدمات ونتحقق منها:

```
root@kali:~# systemctl start hostapd dnsmasq
root@kali:~# systemctl status hostapd dnsmasq
● hostapd.service - LSB: Advanced IEEE 802.11 management daemon
   Loaded: loaded (/etc/init.d/hostapd; generated; vendor preset: disabled)
   Active: active (running) since Mon 2017-08-14 19:24:43 UTC; 2s ago
```

```
[...]

● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server

   Loaded: loaded (/lib/systemd/system/dnsmasq.service; disabled; vendor preset:

   Active: active (running) since Mon 2017-08-14 19:24:43 UTC; 2s ago
```

ولتمكنها للعمل بعد إعادة الإقلاع:

```
root@kali:~# systemctl enable hostapd dnsmasq

hostapd.service is not a native service, redirecting to systemd-sysv-install.

Executing: /lib/systemd/systemd-sysv-install enable hostapd

Synchronizing state of dnsmasq.service with SysV service script with /lib/systemd/systemd-sysv-install.

Executing: /lib/systemd/systemd-sysv-install enable dnsmasq
```

أخيرًا، أعد التشغيل وتأكد من الالتزام بالقواعد بعد إعادة التشغيل. بمجرد إعادة التشغيل، يجب أن تكون قادرًا على الاتصال بـ "Kali Pi" والتصفح!

تمرين الشهادة للفصل الخامس

١. بأي أداة يمكنك التحكم في الشبكة في الواجهة الرسومية لـ gnome؟

- ifupdown
- systemctl
- NetworkManager
- /etc/network/interfaces

٢. يعد ملف الواجهات جزءًا مهمًا من تكوين الشبكة بسطر الأوامر. ما هو المجلد الخاص بها؟

- /etc/networks
- /etc/init.d
- /etc/network
- /etc/init

٣. ما هو اسم حزمة سطر الأوامر المستخدمة عادة في كالي لتكوين الشبكة من سطر الأوامر؟

- systemctl
- init.d
- ifupdown
- hosts

٤. عند تكوين شبكة من سطر الأوامر (على سبيل المثال مع ifup أو ifdown) أي سطر سيبدأ القسم لتكوين شبكة يدوي؟

- o iface eth0 inet auto
- o iface eth0 inet auto
- o iface eth0 inet auto
- o iface eth0 inet static

٥. ما هي الأساليب التي يمكن استخدامها لتكوين أجهزة الشبكة في Kali Linux؟ اختر كل ما يمكن تطبيقه:

- o رسوميا باستخدام NetworkManager
- o بسطر الأوامر باستخدام ملفات network. في المجلد /etc/system/network/
- o بسطر الأوامر بواسطة ملف /etc/network/interfaces/
- o بسطر الأوامر بواسطة systemd-networkd
- o بسطر الأوامر باستخدام ifupdown

٦. أي ملف يحتوي على كلمات مرور المستخدم المشفرة؟

- o /etc/group
- o /etc/shadow
- o /etc/passwd
- o لاشيء مما سبق

٧. ما هو الأمر المستخدم لإضافة مستخدمين؟

- o passwd -l
- o adduser
- o chuser
- o useradd

٨. ما هو الأمر الذي سيعلق حساب المستخدم؟

- o **useradd -s** *olduser*
- o **passwd -l** *olduser*
- o **passwd -s** *olduser*
- o **rmuser -l** *olduser*

٩. ما هو الصحيح لخدمة SSH على تثبيت كالي الافتراضي؟ اختر كل ما ينطبق.

☐ يتم إنشاء المفاتيح الإفتراضية من صورة مباشرة مسبقا

☐ يحظر التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى كلمة المرور

☐ يحظر ملف التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى الشهادات

☐ تم تعطيل خدمة SSH بشكل افتراضي

☐ يتم تثبيت خدمة SSH بشكل افتراضي

١٠. ما هو الأمر الشائع استخدامه لبدء تشغيل خدمات مثل ssh و postgresql؟

- o service
- o systemctl
- o init
- o run

١١. ما هو الأمر المستخدم لإضافة قاعدة بيانات postgresql جديدة؟

- dropdb
- createdb
- psql -n
- db_create

١٢. أي من هذه الأوامر ليس من أوامر postgresql؟

- createuser
- pg_createuser
- psql
- createdb

١٣. أي من هذه الأوامر تنشئ قاعدة بيانات postgres باسم db_new؟

- psql -h localhost -c db_new -O dbuser dbuser
- createdb -T template0 -E UTF-8 -O dbuser db_new
- pg_create -o dbuser -n db_new -E UTF-8
- createdb -T template0 -E UTF-8 -n db_new

١٤. أي مما يلي ليس لها علاقة بـ Apache2؟ اختر واحدة.

- a2enmod
- systemctl start apache
- /etc/apache2
- /var/www/html

١٥. أي مما يلي ليس له علاقة بـ Apache2؟

- /etc/apache2/mods-available
- /etc/apache2/ports.conf
- DocumentRoot
- htpasswd
- .htaccess
- Apachectl

١٦. في كالي، ما هو المسؤول عن تسلسل الإقلاع، ولكنه يعمل أيضًا بصفة دائمة كمدير خدمة كامل الميزات وبدء الخدمات ومراقبتها؟

- init.d
- systemd
- grub
- systemctl

١٧. أي أمر سيفحص الوضع الحالي لخدمة postgresql؟

```
o /etc/init/postgresql status
o ps | grep postgresql
o sudo status postgresql
o systemctl status postgresql
```

الإجابات الصحيحة:

1. NetworkManager
2. /etc/network
3. ifupdown
4. iface eth0 inet static
5. On the command line with .network files in the /etc/systemd/network directory

   On the command line with ifupdown

   On the command line via the /etc/network/interfaces file

   Graphically with NetworkManager

   On the command line with systemd-networkd
6. /etc/shadow
7. **adduser**
8. **passwd -l** *olduser*
9. The SSH service is installed by default

   The default configuration blocks password-based logins

   The SSH service is disabled by default

   The default keys from a live image are pre-generated
10. **systemctl**
11. **createdb**
12. pg_createuser
13. **createdb -T template0 -E UTF-8 -O dbuser db_new**
14. **systemctl start apache**
15. apachectl
16. systemd
17. **systemctl status postgresql**

```
#usermod -a -G group user
```

---((الفصل السادس))---

٦. الحصول على المساعدة

بغض النظر عن عدد سنوات الخبرة التي لديك، فلا شك في أنك ستواجه مشكلة - عاجلاً أم آجلاً. غالبًا ما يكون حل هذه المشكلة مسألة فهمها ثم الاستفادة من الموارد المختلفة لإيجاد حل أو حل بديل.

في هذا الفصل، سنناقش مصادر المعلومات المختلفة المتاحة ونناقش أفضل الاستراتيجيات للعثور على المساعدة التي تحتاجها أو حل المشكلة التي قد تواجهها. سنأخذك أيضًا في جولة في بعض موارد مجتمع Kali Linux المتاحة، بما في ذلك منتديات الويب وقناة Internet Relay Chat (IRC). أخيرًا، سنقدم لك تقريرًا عن الأخطاء وسنوضح لك كيفية الاستفادة من أنظمة حفظ الأخطاء لاستكشاف المشكلات وإصلاحها ووضع استراتيجيات لمساعدتك في تقديم تقرير الأخطاء الخاص بك بحيث يمكن معالجة المشكلات غير الموثقة بسرعة وفعالية.

١.٦. مصادر التوثيق

قبل أن تتمكن من فهم ما يحدث حقًا عند وجود مشكلة، تحتاج إلى معرفة الدور النظري الذي يلعبه كل برنامج مشارك في المشكلة. واحدة من أفضل الطرق للقيام بذلك هي مراجعة وثائق البرنامج. دعنا نبدأ بمناقشة مكان، بالضبط، يمكنك العثور على وثائق لأنها غالبًا ما تكون مبعثرة.

كيفية تجنب إجابات RTFM

يشير هذا الاختصار إلى "Read The F***ing Manual"، ولكن يمكن أيضًا توسيعه بصيغة أكثر ودية، "Read The Fine Manual". تُستخدم هذه العبارة أحيانًا في ردود على أسئلة مبتدئين. إنه أمر مفاجئ إلى حد ما، وينم عن إزعاج معين في سؤال يطرحه شخص لم يكلف نفسه عناء قراءة الوثائق. يقول البعض أن هذه الاستجابة أفضل من عدم الاستجابة على الإطلاق لأن هذا على الأقل يشير إلى أن الإجابة في الوثائق.

عندما تنشر أسئلة، لا تشعر بالضرورة بالإهانة من رد RTFM، ولكن افعل ما بوسعك على الأقل لإثبات أنك قد استغرقت بعض الوقت لإجراء بعض البحث قبل نشر السؤال؛ اذكر المصادر التي استشرتها ووصف الخطوات المختلفة التي اتخذتها شخصيًا للعثور على المعلومات. هذا سيقطع شوطًا طويلًا لإظهار أنك لست كسولًا وتسعى حقًا إلى المعرفة. يُعد اتباع إرشادات Eric Raymond's طريقة جيدة لتجنب الأخطاء الأكثر شيوعًا والحصول على إجابات مفيدة.

http://catb.org/~esr/faqs/smart-questions.html

١.١.٦. الصفحات اليدوية

تحتوي الصفحات اليدوية، بالرغم من كونها قصيرة نسبيًا، على قدر كبير من المعلومات الأساسية. لعرض صفحة يدوية، ما عليك سوى كتابة **man**. عادة ما يكون اسم الوثيقة هو نفس اسم الأمر. على سبيل المثال، للتعرف على الخيارات الممكنة للأمر **cp**، يمكنك كتابة **man cp**.

لا تقوم صفحات Man بتوثيق البرامج التي يمكن الوصول إليها من سطر الأوامر فحسب، بل أيضًا ملفات التكوين ومكالمات النظام ووظائف مكتبة C وما إلى ذلك. في بعض الأحيان يمكن أن تتصادم الأسماء. على سبيل المثال، أمر **read** الخاص بالصدفة له نفس اسم استدعاء نظام القراءة **read**. هذا هو سبب تنظيم الصفحات اليدوية في الأقسام المرقمة التالية:

١. الأوامر التي يمكن تنفيذها من سطر الأوامر

٢. مكالمات النظام (الوظائف التي توفرها النواة)

٣. وظائف المكتبة (تقدمها مكتبات النظام)

٤. الأجهزة (على أنظمة شبيهة بنظام يونكس، هذه ملفات خاصة، توضع عادة في مجلد /dev/)

٥. ملفات التكوين

٦. الألعاب

٧. مجموعات وحدات الماكرو والمعايير

٨. أوامر إدارة النظام

٩. روتينات النواة

يمكنك تحديد قسم الصفحة اليدوية الذي تبحث عنه: لعرض وثائق مكالمة نظام read، يمكنك كتابة man 2 read. عندما لا يتم تحديد أي قسم بشكل صريح، سيتم عرض القسم الأول الذي يحتوي على صفحة يدوية بالاسم المطلوب. وبالتالي، **man shadow** يُرجع (5) shadow لأنه لا توجد صفحات يدوية لـ shadow في الأقسام ١-٤.

بالطبع، إذا كنت لا تعرف أسماء الأوامر، فلن يكون الدليل مفيدًا لك كثيرًا. أدخل الأمر **apropos**، الذي يبحث في الصفحات اليدوية (أو بشكل أكثر تحديدًا وصفها القصير) عن أي كلمات رئيسية تقدمها. يقوم الأمر **apropos** بعد ذلك بإرجاع قائمة بالصفحات اليدوية التي يذكر ملخصها الكلمات الرئيسية المطلوبة جنبًا إلى جنب مع الملخص المكون من سطر واحد من الصفحة اليدوية. إذا اخترت كلماتك الرئيسية جيدًا، فستجد اسم الأمر الذي تحتاجه.

مثال ١.٦. إيجاد **cp** بواسطة الأمر **apropos**

```
$ apropos "copy file"
cp (1)               - copy files and directories
cpio (1)             - copy files to and from
archives
gvfs-copy (1)        - Copy files
gvfs-move (1)        - Copy files
hcopy (1)            - copy files from or to an HFS
volume
install (1)          - copy files and set attributes
ntfscp (8)           - copy file to an NTFS volume.
```

تصفح الوثائق باتباع الروابط

تحتوي العديد من الصفحات اليدوية على قسم "انظر أيضًا"، عادةً بالقرب من نهاية المستند، والذي يشير إلى الصفحات اليدوية الأخرى ذات الصلة بالأوامر المماثلة، أو الوثائق الخارجية. يمكنك استخدام هذا القسم للعثور على الوثائق ذات الصلة حتى عندما لا يكون الخيار الأول هو الأمثل.

بالإضافة إلى **man**، يمكنك استخدام **konqueror** (في KDE) و **yelp** (في GNOME) للبحث في صفحات man أيضًا.

٢.١.٦. وثائق المعلومات info

لقد كتب مشروع GNU أدلة لأغلب برامجه بصيغة المعلومات info، هذا هو السبب في أن العديد من الصفحات اليدوية تشير إلى وثائق المعلومات المقابلة. يقدم هذا التنسيق بعض الميزات ولكن البرنامج الافتراضي لعرض هذه المستندات (يسمى أيضًا **info**) أكثر تعقيدًا بعض الشيء. ننصحك باستخدام **pinfo** (من حزمة pinfo) بدلا من ذلك. لتثبيته، ما عليك سوى تشغيل **apt update** متبوعًا بـ **apt install pinfo** (انظر القسم ٢.٢.٢.٨، "تثبيت الحزم باستخدام APT").

تحتوي وثائق المعلومات على هيكل هرمي وإذا قمت باستدعاء **pinfo** بدون معلمات، فسوف تعرض قائمة بالعُقد المتوفرة في المستوى الأول. عادة، تحمل العقد اسم الأوامر المقابلة.

يمكنك استخدام مفاتيح الأسهم للتنقل بين العقد. بدلاً من ذلك، يمكنك أيضًا استخدام متصفح رسومي (وهو أكثر سهولة في الاستخدام) مثل **konqueror** أو **yelp**.

فيما يتعلق بترجمات اللغة، يكون نظام المعلومات دائمًا باللغة الإنجليزية وغير مناسب للترجمة، على عكس صفحات **man**. ومع ذلك، عندما تطلب من برنامج **pinfo** عرض صفحة معلومات غير موجودة، فسوف تعود إلى صفحة *الدليل* بنفس الاسم (إن وجد)، والتي قد تتم ترجمتها.

٣.١.٦. وثائق خاصة بالحزمة

تحتوي كل حزمة على الوثائق الخاصة بها، وحتى أقل البرامج توثيقًا بشكل عام تحتوي على ملف README يحتوي على بعض المعلومات المهمة و/أو المهمة. يتم تثبيت هذه الوثائق في المجلد **/usr/share/doc/***package*/ (حيث يمثل *package* اسم الحزمة). إذا كانت الوثائق كبيرة بشكل خاص، فقد لا يتم تضمينها في الحزمة الرئيسية للبرنامج، ولكن قد يتم إلغاء تحميلها إلى حزمة مخصصة تسمى عادةً *package*-**doc**. توصي الحزمة الرئيسية عمومًا بحزمة التوثيق بحيث يمكنك العثور عليها بسهولة.

يحتوي المجلد **/usr/share/doc/***package*/ على بعض الملفات المقدمة من دبيان، والتي تكمل الوثائق من خلال تحديد خصائص الحزمة أو التحسينات مقارنة بالتثبيت التقليدي للبرنامج. يشير ملف **README.Debian** أيضًا إلى جميع التعديلات التي تم إجراؤها لتتوافق مع سياسة دبيان. يسمح ملف **changelog.Debian.gz** للمستخدم باتباع التعديلات التي أدخلت على الحزمة بمرور الوقت؛ من المفيد جدًا محاولة فهم ما تغير بين نسختين مثبتتين ليس لهما نفس السلوك. أخيرًا، يوجد أحيانًا ملف **NEWS.Debian.gz** يوثق التغييرات الرئيسية في البرنامج التي قد تهم المسؤول بشكل مباشر.

٤.١.٦. مواقع الويب

في كثير من الحالات، يمكنك العثور على مواقع الويب التي يتم استخدامها لتوزيع برامج مجانية ولجمع مجتمع مطوريها ومستخدميها. يتم تحميل هذه المواقع بالمعلومات ذات الصلة في أشكال مختلفة مثل الوثائق الرسمية والأسئلة الشائعة "frequently asked questions"(FAQ) وأرشيفات القوائم البريدية. في معظم الحالات، تعالج أرشيفات الأسئلة الشائعة أو أرشيف القوائم البريدية المشكلات التي واجهتها. أثناء البحث عن المعلومات عبر الإنترنت، من المفيد للغاية إتقان بنية البحث. نصيحة سريعة: حاول قصر البحث على نطاق معين، مثل النطاق المخصص للبرنامج الذي يسبب لك المشاكل. إذا أعاد البحث عددًا كبيرًا جدًا من الصفحات أو إذا لم تتطابق النتائج مع ما تبحث عنه، فيمكنك إضافة الكلمة الرئيسية **kali** أو **debian** للحد من النتائج واستهداف المعلومات ذات الصلة.

من المشلكة للحل

إذا أعاد البرنامج رسالة خطأ محددة للغاية، فأدخلها في محرك بحث (بين علامتي اقتباس مزدوجتين "، للبحث عن العبارة الكاملة، بدلاً من الكلمات الرئيسية الفردية). في معظم الحالات، ستحتوي الروابط الأولى التي تم إرجاعها على الإجابة التي تحتاجها. في حالات أخرى، ستحصل على أخطاء عامة جدًا، مثل "تم رفض الإذن". في هذه الحالة، من الأفضل التحقق من أذونات العناصر المعنية (الملفات، معرف المستخدم، المجموعات، إلخ). باختصار، لا تعتاد دائمًا استخدام محرك بحث لإيجاد حل لمشكلتك. ستجد أنه من السهل جدًا نسيان استخدام الحس السليم.

إذا كنت لا تعرف عنوان موقع البرنامج، فهناك العديد من الوسائل لتحديد موقعه. أولاً، ابحث عن حقل الصفحة الرئيسية "Home page" في المعلومات الوصفية للحزمة (**apt show** *package*). بدلاً من ذلك، قد يحتوي وصف الحزمة على رابط إلى موقع الويب الرسمي للبرنامج.

إذا لم يتم تحديد عنوان URL، فربما يكون مشرف الحزمة قد ضمّن عنوان URL في ملف **/usr/share/doc/***package***/Copyright**. أخيرًا، قد تتمكن من استخدام محرك بحث (مثل Google و DuckDuckGo و Yahoo وما إلى ذلك) للعثور على موقع البرنامج.

٥.١.٦. وثائق كالي في docs.kali.org

يحتفظ مشروع كالي بمجموعة من الوثائق المفيدة على http://docs.kali.org. على الرغم من أن هذا الكتاب يغطي جزءًا كبيرًا مما يجب أن تعرفه عن Kali Linux، فقد لا تزال الوثائق هناك مفيدة لأنها تحتوي على إرشادات خطوة بخطوة (مثل الكثير من الإرشادات) حول العديد من الموضوعات.

http://docs.kali.org/

دعنا نراجع الموضوعات المختلفة التي يتم تناولها هناك:

- ❖ الشروع في العمل: سلسلة من التعليمات، بما في ذلك تعليمات التنزيل، لأولئك الجدد على Kali
- ❖ Kali Linux Live: وثائق تصف كيفية استخدام Kali Linux كنظام مباشر
- ❖ تثبيت Kali Linux: وثائق مختلفة تصف تثبيت Kali Linux، بما في ذلك كيفية تثبيته جنبًا إلى جنب مع أنظمة التشغيل الأخرى
- ❖ Kali Linux على ARM: العديد من الوصفات حول تشغيل Kali Linux على مختلف الأجهزة القائمة على ARM
- ❖ استخدام Kali Linux: العديد من الإرشادات حول العديد من الطلبات الشائعة

- ❖ تخصيص Kali Linux: تعليمات للمتعبين الذين يرغبون في إعادة بناء Kali بناءً على متطلباتهم الخاصة
- ❖ Kali Community Support: يشير إلى المجتمعات المختلفة حيث يمكنك الحصول على الدعم والتوضيحات حول كيفية إرسال تقارير الأخطاء
- ❖ سياسات Kali Linux: توضيحات حول ما يجعل Kali Linux مميزًا عند مقارنته بتوزيعات Linux الأخرى
- ❖ The Kali Linux Dojo: مقاطع فيديو لورشات Black Hat و DEF CON

٢.٦. مجتمعات كالي لينكس

هناك العديد من مجتمعات Kali Linux حول العالم تستخدم العديد من الأدوات المختلفة للتواصل (المنتديات والشبكات الاجتماعية، على سبيل المثال). في هذا القسم، سنقدم فقط مجتمعين رسميين لـ Kali Linux.

١.٢.٦. منتديات الويب على forums.kali.org

توجد منتديات المجتمع الرسمية لمشروع كالي لينكس على forums.kali.org. مثل كل منتدى قائم على الويب، يجب عليك إنشاء حساب لتتمكن من النشر ويتذكر النظام ما هي المنشورات التي رأيتها بالفعل، مما يجعل من السهل متابعة المحادثات على أساس منتظم.

قبل النشر، يجب عليك قراءة قواعد المنتدى:

http://docs.kali.org/community/kali-linux-community-forums

لن نقوم بكتابتها هنا ولكن تجدر الإشارة إلى أنه لا يُسمح لك بالتحدث عن الأنشطة غير القانونية مثل اختراق شبكات الأشخاص الآخرين. يجب أن تكون محترمًا لأعضاء المجتمع الآخرين لإنشاء مجتمع ترحيبي. الإعلان محظور ويجب تجنب المناقشات خارج الموضوع. هناك فئات كافية لتغطية كل شيء تود مناقشته حول Kali Linux.

٢.٢.٦. # قناة kali linux IRC على Freenode

IRC هو نظام دردشة في الوقت الحقيقي. تحدث المناقشات في غرف الدردشة التي تسمى القنوات وعادة ما تتمحور حول موضوع أو مجتمع معين. يستخدم مشروع Kali Linux قناة #kali-linux على شبكة Freenode (يمكنك استخدام chat.freenode.net كخادم IRC، على المنفذ 6667 لاتصال مشفر بـ TLS أو منفذ 6666 لاتصال نص واضح).

للانضمام إلى المناقشات حول IRC، يجب عليك استخدام عميل IRC مثل **hexchat** (في الوضع الرسومي) أو **irssi** (في وضع وحدة التحكم). يتوفر أيضًا عميل قائم على الويب على webchat.freenode.net.

في حين أنه من السهل حقًا الانضمام إلى المحادثة، يجب أن تكون على دراية بأن قنوات IRC لها قواعدها الخاصة وأن هناك عوامل تشغيل للقنوات (يُطلق لقبهم بـ @) يمكنهم فرض القواعد: يمكنهم طردك من القناة (أو حتى منعك إذا استمرت في عصيان القواعد). قناة #kali-linux ليست استثناء. تم توثيق القواعد هنا:

http://docs.kali.org/community/kali-linux-irc-channel

لتلخيص القواعد: يجب أن تكون ودودًا ومتسامحًا ومعقولًا. يجب تجنب المناقشات خارج الموضوع. على وجه الخصوص، يحظر المناقشات حول الأنشطة غير القانونية /الثغرات/البرمجيات المقرصنة، والسياسة، والأديان. ضع في اعتبارك أن عنوان IP الخاص بك سيكون متاحًا للآخرين.

إذا كنت تريد طلب المساعدة، فاتبع التوصيات الواردة في كيفية تجنب إجابات RTFM: قم بإجراء بحثك أولاً وشارك النتائج. عندما يُطلب منك معلومات تكميلية، يرجى تقديمها بدقة (إذا كان عليك تقديم بعض الإخراج المطول، فلا تلصقها في القناة مباشرة، وبدلاً من ذلك استخدم خدمة مثل Pastebin ونشر عنوان URL الخاص بـ Pastebin فقط).

لا تتوقع إجابة فورية. على الرغم من أن IRC هو منصة اتصال في الوقت الفعلي، إلا أن المشاركين يسجلون الدخول من جميع أنحاء العالم، لذلك تختلف المناطق الزمنية وجداول العمل. قد يستغرق الرد على سؤالك بضع دقائق أو ساعات. ومع ذلك، عندما يدرج الآخرون لقبك في الرد، سيتم تمييز لقبك وسوف يخطرك (إشعار) معظم عملاء IRC، لذا اترك عميلك متصلاً وتحلى بالصبر.

```
/*
$ sudo apt install irssi
$ irssi
/connect chat.freenode.net
/join #kali-linux
```

للمزيد قم بتنزيل الملف:

```
https://bit.ly/irssi_tool
*/
```

٣.٦. تقديم تقرير خطأ جيد

إذا فشلت كل جهودك لحل المشكلة، فمن المحتمل أن تكون المشكلة بسبب خطأ في البرنامج. في هذه الحالة، ربما أدت المشكلة إلى تقرير خطأ. يمكنك البحث عن تقارير الأخطاء لإيجاد حل لمشكلتك ولكن دعنا نلقي نظرة على إجراء الإبلاغ عن خطأ إلى Kali أو Debian أو مباشرة إلى مطوري البرنامج حتى تفهم العملية إذا كنت بحاجة إلى إرسال تقريرك الخاص.

الهدف من تقرير الخطأ هو توفير معلومات كافية حتى يتمكن مطورو أو مشرفو البرنامج المعيب (المفترض) من إعادة إنتاج المشكلة وتصحيح سلوكها وتطوير حل لها. هذا يعني أن تقرير الخطأ الخاص بك يجب أن يحتوي على معلومات مناسبة ويجب توجيهه إلى الشخص الصحيح أو فريق المشروع. يجب أن يكون التقرير مكتوبًا بشكل جيد وشاملًا، مما يضمن استجابة أسرع.

يختلف الإجراء الدقيق لتقرير الخطأ اعتمادًا على المكان الذي سترسل فيه التقرير (Kali، Debian، upstream developer) ولكن هناك بعض التوصيات العامة التي تنطبق على جميع الحالات. في هذا الفصل سوف نناقش تلك التوصيات.

٦.٣.١. توصيات عامة

دعنا نناقش بعض التوصيات العامة والمبادئ التوجيهية التي ستساعدك على إرسال تقرير خطأ واضح وشامل ويحسن فرص معالجة المطورين من قبل المطورين في الوقت المناسب.

٦.٣.١.١. كيفية التواصل

اكتب تقريرك باللغة الإنجليزية

ما لم تكن تعرف محادثك، فيجب أن تستخدم لغة إنجليزية بسيطة. إذا كنت متحدثًا أصليًا للغة الإنجليزية، فاستخدم جملًا بسيطة وتجنب الإنشاءات التي قد يصعب فهمها للأشخاص ذوي مهارات محدودة في اللغة الإنجليزية. على الرغم من أن معظم المطورين يتمتعون بذكاء كبير، إلا أن ليس لديهم كلًا مهارات قوية في اللغة الإنجليزية. من الأفضل ألا تفترض.

احترم عمل المطورين

تذكر أن معظم مطوري البرمجيات الحرة (بما في ذلك أولئك الذين يقفون وراء Kali Linux) هم خيرين ويقضون وقت فراغهم المحدود للعمل على البرنامج الذي تستخدمه بحرية. يفعل الكثيرون ذلك بدافع الإيثار. وبالتالي، عندما تقدم تقريرًا عن خطأ، كن محترمًا (حتى لو بدا الخطأ كخطأ واضح من المطور) ولا تفترض أنهم مدينون لك بإصلاح. نشكرهم على مساهمتهم بدلاً من ذلك.

إذا كنت تعرف كيفية تعديل البرنامج وإعادة ترجمته، اعرض مساعدة المطورين في اختبار أي تصحيحات يرسلونها إليك. سيظهر لهم ذلك أنك على استعداد لاستثمار وقتك أيضًا.

كن متفاعلًا وجاهزًا لتقديم المزيد من المعلومات

في بعض الحالات، سيرجع المطور إليك بطلبات للحصول على مزيد من المعلومات أو طلبات لمحاولة إعادة إنشاء المشكلة ربما باستخدام خيارات مختلفة أو باستخدام حزمة محدثة. يجب أن تحاول الرد على هذه الاستفسارات في أسرع وقت ممكن. كلما أرسلت ردك بشكل أسرع، زادت فرصة تمكنهم من حلها بسرعة بينما لا يزال التحليل الأولي جديدًا في أذهانهم.

بينما يجب أن تهدف إلى الاستجابة بسرعة، يجب ألا تسير بسرعة كبيرة: يجب أن تكون البيانات المقدمة صحيحة ويجب أن تحتوي على كل ما طلبه المطورون. سيشعرون بالانزعاج إذا اضطروا لطلب شيء ما مرة أخرى.

٢.١.٣.٦. ما يجب وضعه في تقرير الخطأ

تعليمات إعادة إنتاج المشكلة

لكي تتمكن من إعادة إظهار المشكلة، يحتاج المطورون إلى معرفة ما تستخدمه، ومن أين حصلت عليه، وكيف قمت بتثبيته.

يجب عليك تقديم تعليمات دقيقة خطوة بخطوة تصف كيفية إعادة إظهار المشكلة. إذا كنت بحاجة إلى استخدام بعض البيانات لإعادة إظهار المشكلة، فقم بإرفاق الملف المقابل بتقرير الخطأ. حاول التوصل إلى الحد الأدنى من التعليمات اللازمة لإعادة إنتاج الخطأ.

قدم بعض السياق وحدد توقعاتك

اشرح ما كنت تحاول القيام به وكيف توقعت أن يتصرف البرنامج.

في بعض الحالات، يظهر لك الخطأ فقط لأنك كنت تستخدم البرنامج بطريقة لم يتم تصميمه لها.

في بعض الحالات الأخرى، قد يكون السلوك الذي تصفه بأنه خطأ هو السلوك العادي. كن صريحًا بشأن ما كنت تتوقع أن يفعله البرنامج. هذا سيوضح الوضع للمطورين. يمكنهم إما تحسين السلوك أو تحسين التوثيق، لكي يعرفوا على الأقل أن سلوك برنامجهم يربك بعض المستخدمين!

كن دقيقا

قم بتضمين أرقام إصدارات البرنامج التي تستخدمها، ربما مع أرقام إصدارات تبعياتها. عندما تشير إلى شيء قمت بتنزيله، قم بتضمين عنوان URL الكامل الخاص به.

عندما تتلقى رسالة خطأ، اقتبسها تمامًا كما رأيتها. إن أمكن، ضمّن نسخة من إخراج الشاشة أو لقطة شاشة. ضمّن نسخة من أي ملف سجل ذي صلة، مع التأكد من إزالة أي بيانات حساسة أولاً.

اذكر الإصلاحات الممكنة أو الحلول البديلة

قبل تقديم تقرير الخطأ، ربما حاولت حل المشكلة. اشرح ما حاولت القيام به وما النتائج التي تلقيتها. كن واضحًا جدًا بشأن ما هي الحقيقة وما هي مجرد فرضية من جانبك.

إذا أجريت بحثًا عبر الإنترنت ووجدت بعض التفسيرات حول مشكلة مشابهة، فيمكنك ذكرها، لا سيما عندما تجد تقارير أخطاء مشابهة أخرى في أداة تتبع الأخطاء في دبيان أو في أداة تتبع الأخطاء الأولية.

إذا وجدت طريقة لتحقيق النتيجة المرجوة دون تشغيل الخطأ، يرجى توثيق ذلك أيضًا. سيساعد هذا المستخدمين الآخرين الذين تضرروا من نفس المشكلة.

تقارير الأخطاء الطويلة جيدة

تقرير خلل من سطرين غير كاف؛ يتطلب تقديم جميع المعلومات المطلوبة عادةً عدة فقرات (أو أحيانًا صفحات) من النص.

قدم كل المعلومات التي تستطيع. حاول الالتزام بما هو مناسب، ولكن إذا لم تكن متأكدًا، فالكثير أفضل من القليل.

إذا كان تقرير الخطأ الخاص بك طويلًا حقًا، خصص بعض الوقت لتنظيم المحتوى وتقديم ملخص قصير في البداية.

٣.١.٣.٦. نصائح متنوعة

تجنب تقديم تقارير الأخطاء المكررة

في عالم البرمجيات الحرة، جميع أجهزة تتبع الأخطاء عامة. يمكن تصفح المشكلات المفتوحة ولديها ميزة البحث. وبالتالي، قبل تقديم تقرير خطأ جديد، حاول تحديد ما إذا كان شخص آخر قد أبلغ بالفعل عن مشكلتك.

إذا عثرت على تقرير خطأ حالي، اشترك فيه وربما أضف معلومات تكميلية. لا تنشر تعليقات مثل "أنا أيضًا" أو "+١"، لأنها لا تنفع بشيء. ولكن يمكنك الإشارة إلى أنك متاح لمزيد من الاختبارات إذا لم يقدم مقدم الطلب الأصلي ذلك.

إذا لم تعثر على أي تقرير عن مشكلتك، فانتقل وأرسلها. إذا تقرير ذي صلة، فتأكد من ذكرها.

تأكد من استخدام أحدث إصدار

إنه لأمر محبط للغاية أن يتلقى المطورون تقارير أخطاء عن المشكلات التي قاموا بحلها بالفعل أو المشكلات التي لا يمكنهم إعادة إنتاجها باستخدام الإصدار الذي يستخدمونه (غالبًا ما يستخدم المطورون أحدث إصدار من منتجهم). حتى عندما يتم الاحتفاظ بالإصدارات القديمة من قبل المطورين، غالبًا ما يقتصر الدعم على إصلاحات الأمان والمشكلات الرئيسية. هل أنت متأكد من أن الخلل الخاص بك هو واحد من هذه الأخطاء؟

لهذا السبب، قبل تقديم تقرير الأخطاء، يجب عليك التأكد من أنك تستخدم أحدث إصدار من النظام والتطبيق الإشكالي وأنه يمكنك إعادة إنتاج المشكلة في هذا الموقف.

إذا كان Kali Linux لا يقدم أحدث إصدار من التطبيق (لا في kali-rolling ولا في kali-bleeding-edge، راجع القسم ٣.٣.١.٨، "مستودع Kali-Bleeding-Edge")، فلديك حلول بديلة: يمكنك تجريبها جرب التثبيت اليدوي لأحدث إصدار في جهاز افتراضي، أو يمكنك مراجعة سجل التغيير ChangeLog (أو سجل تنفيذ Git) لمعرفة أنه لم يكن هناك أي تغيير يمكن أن يحل المشكلة التي تراها (وثم قم بإيداع الخطأ حتى لو لم تجرب أحدث إصدار).

لا تخلط مشكلات متعددة في تقرير خطأ واحد

إرسال تقرير خطأ واحد لكل مشكلة. بهذه الطريقة، لا تصبح المناقشات اللاحقة فوضوية للغاية ويمكن إصلاح كل خطأ وفقًا لجدوله الزمني. إذا لم تفعل ذلك، فإما أن يكون الخطأ الواحد بحاجة إلى إعادة تعيين الغرض منه عدة مرات ولا يمكن إغلاقه إلا بعد إصلاح جميع المشكلات، أو يجب على المطورين تقديم التقارير التكميلية التي كان عليك إنشاؤها في المقام الأول.

٢.٣.٦. مكان تقديم تقرير خطأ

لتتمكن من تحديد مكان إرسال تقرير الخطأ، يجب أن يكون لديك فهم جيد للمشكلة ويجب أن تكون قد حددت أي جزء من البرنامج تكمن فيه المشكلة.

من الناحية المثالية، تتبع المشكلة وصولاً إلى ملف على نظامك ثم يمكنك استخدام **dpkg** لمعرفة الحزمة التي تمتلك هذا الملف ومن أين تأتي هذه الحزمة. لنفترض أنك عثرت على خطأ في تطبيق رسومي. بعد الاطلاع على قائمة العمليات الجارية (مخرجات **ps auxf**)، اكتشفت أن التطبيق بدأ باستخدام الملف التنفيذي **usr/bin/sparta/** القابل للتنفيذ:

```
$ dpkg -S /usr/bin/sparta</code> sparta:
/usr/bin/sparta
$ dpkg -s sparta | grep ^Version: Version:
1.0.1+git20150729-0kali1
```

أنت تعلم أن**usr/bin/sparta/** يتم توفيره بواسطة حزمة **sparta**، والتي توجد في الإصدار ١.٠.١ + git20150729-0kali1. تشير حقيقة أن سلسلة الإصدار تحتوي على kali إلى أن الحزمة تأتي من Kali Linux (أو معدلة بواسطة Kali Linux). أي حزمة لا تحتوي على كالي في سلسلة نسختها (أو في اسم الحزمة) تأتي مباشرة من دبيان (اختبار دبيان بشكل عام).

تحقق مرة أخرى قبل إيداع الأخطاء ضد دبيان

إذا وجدت خطأ في حزمة مستوردة مباشرة من دبيان، فمن الأفضل الإبلاغ عنها وإصلاحها في جانب دبيان. ومع ذلك، قبل القيام بذلك، تأكد من أن المشكلة قابلة للتكرار على نظام دبيان العادي لأن كالي ربما تسبب في المشكلة عن طريق تعديل الحزم أو التبعيات الأخرى.

أسهل طريقة لتحقيق ذلك هي إعداد جهاز افتراضي يعمل على Debian Testing. يمكنك العثور على تثبيت صورة ISO لـ Debian Testing على موقع Debian Installer:

https://www.debian.org/devel/debian-installer/

إذا تمكنت من تأكيد المشكلة في الجهاز الإفتراضي، فيمكنك إرسال الخطأ إلى دبيان عن طريق تشغيل **reportbug** داخل الجهاز الإفتراضي واتباع التعليمات المقدمة.

يجب توجيه معظم تقارير الأخطاء حول سلوك التطبيقات إلى مشروعات المنبع الخاصة بها إلا عند مواجهة مشكلة في التكامل: في هذه الحالة، يعد الخطأ خطأ في طريقة حزم البرنامج ودمجه في دبيان أو كالي. على سبيل المثال، إذا كان أحد التطبيقات يوفر خيارات وقت الترجمة التي لا تمكّنها الحزمة أو لا يعمل التطبيق بسبب عدم وجود مكتبة (وبالتالي تسليط الضوء على تبعية مفقودة في المعلومات الوصفية للحزمة)، فقد تواجه تكاملًا مشكلة. عندما لا تعرف نوع المشكلة التي تواجهها، فمن الأفضل عادةً تقديم المشكلة على كلا الجانبين والإحالة إليها.

عادة ما يكون تحديد مصدر المشروع والعثور على مكان تقديم تقرير الخطأ أمرًا سهلاً. عليك فقط تصفح موقع المصدر، والذي تمت الإشارة إليه في حقل **Homepage** للبيانات الوصفية للتعبئة:

```
$ dpkg -s sparta | grep ^Homepage:
Homepage: https://github.com/SECFORCE/sparta
```

٦.٣.٣. كيفية تقديم تقرير خطأ

٦.٣.٣.١. تقديم تقرير خطأ في كالي

يستخدم Kali أداة تتبع الأخطاء المستندة إلى الويب على http://bugs.kali.org حيث يمكنك استشارة جميع تقارير الأخطاء بشكل مجهول، ولكن إذا كنت ترغب في التعليق أو تقديم تقرير خطأ جديد، فستحتاج إلى تسجيل حساب.

٦.٣.٣.١.١. الاشتراك في حساب Bug Tracker

للبدء، ما عليك سوى النقر فوق Signup for new account على موقع bug tracker "تتبع الأخطاء"، كما هو موضح في الشكل ٦.١. "الصفحة الرئيسية لتتبع الأخطاء في Kali".

شكل ٦.١. الصفحة الرئيسية لتتبع الأخطاء في Kali

بعد ذلك، قدم اسم مستخدم وعنوان بريد إلكتروني واستجابة لتحدي CAPTCHA. ثم انقر فوق زر **Signup** للمتابعة (الشكل ٢.٦، "صفحة التسجيل").

KALI LINUX
BUG TRACKER

Signup

Username:	NewBugSubmitter
E-mail:	nbs@email.com
Enter the code as it is shown in the box on the right.:	ABFF1

On completion of this form and verification of your answers, you will be sent a confirmation e-mail to the e-mail address you specified.
Using the confirmation e-mail, you will be able to activate your account. If you fail to activate your account within seven days, it will be purged.
You must specify a valid e-mail address in order to receive the account confirmation e-mail.

Signup

[Login] [Lost your password?]

شكل ٢.٦، صفحة التسجيل

إذا نجحت، ستعلمك الصفحة التالية (الشكل ٣.٦، "صفحة تأكيد التسجيل") بأنه تمت معالجة تسجيل الحساب، وسوف يرسل نظام تعقب الأخطاء رسالة بريد إلكتروني للتأكيد من العنوان الذي قدمته. ستحتاج إلى النقر فوق الرابط الموجود في البريد الإلكتروني لتفعيل حسابك.

بمجرد تنشيط حسابك، انقر فوق **Proceed** للمتابعة إلى صفحة تسجيل دخول متعقب الأخطاء.

KALI LINUX
BUG TRACKER

Account registration processed.

Congratulations, you have registered successfully ! You are now being sent a confirmation e-mail to verify your e-mail address. Visiting the link sent to you in this e-mail will activate your account.

You have seven days to complete the account confirmation process; if you fail to do so within this period, the newly-registered account may be purged.

[Proceed]

شكل ٣.٦. صفحة تأكيد التسجيل

٢.١.٣.٣.٦. إنشاء التقرير

لبدء تقريرك، قم بتسجيل الدخول إلى حسابك وانقر على رابط الإبلاغ عن مشكلة على الصفحة المقصودة. سيتم تقديم نموذج مع العديد من الحقول للملئ، كما هو موضح في الشكل ٤.٦. "نموذج للإبلاغ عن خطأ".

Enter Report Details	
*Category	[All Projects] Kali Package Bug
Reproducibility	have not tried
Severity	minor
Priority	normal
Product Version	
*Summary	
*Description	
Steps To Reproduce	
Additional Information	
Upload File (Maximum size: 2,097k)	Parcourir... Aucun fichier sélectionné.
View Status	public private
Report Stay	check to report more issues
* required	Submit Report

شكل ٤.٦. نموذج للإبلاغ عن خطأ

فيما يلي قائمة بجميع الحقول في النموذج:

الفئة "Category" (إلزامية)

يصف هذا الحقل فئة الخطأ الذي ترسله. التقارير التي يمكن أن تعزى إلى حزمة معينة يجب أن تودع في فئات Kali Package Bug أو Kali Package Improvement. يجب أن تستخدم التقارير الأخرى فئات الأخطاء العامة أو طلبات الميزات. الفئات المتبقية مخصصة لحالات استخدام محددة: يمكن استخدام ترقية الأداة لإعلام مطوري Kali بتوافر إصدار جديد من برنامج تم حزمه في Kali. يمكن استخدام طلبات الأدوات الجديدة لاقتراح أدوات جديدة للتعبئة ودمجها في توزيعة كالي.

قابلية اعادة الأنتاج "Reproducibility"

يوثق هذا الحقل ما إذا كانت المشكلة قابلة للتكرار بطريقة يمكن التنبؤ بها أو إذا حدثت بشكل عشوائي إلى حد ما.

الشدة والأولوية "Severity and Priority"

من الأفضل ترك هذه الحقول دون تعديل لأنها مخصصة بشكل أساسي للمطورين. يمكنهم استخدامها لفرز قائمة القضايا حسب شدة المشكلة والأولوية التي يجب التعامل معها.

إصدار المنتج "Product Version"

يجب أن يشير هذا الحقل إلى إصدار Kali Linux الذي تقوم بتشغيله (أو الإصدار الأقرب إلى ما تقوم بتشغيله). فكر مرتين قبل الإبلاغ عن مشكلة في إصدار قديم لم يعد مدعومًا.

ملخص "Summary" (إلزامي)

هذا هو في الأساس عنوان تقرير الخطأ الخاص بك وهو أول شيء يراه الناس. تأكد من أنه يبين سبب تقديم التقرير. تجنب الأوصاف العامة مثل "X لا يعمل" واختر بدلاً من ذلك "X فشل مع الخطأ Y تحت الشرط Z".

الوصف "Description" (إلزامي)

هذا هو نص تقريرك. هنا يجب عليك إدخال جميع المعلومات التي جمعتها حول المشكلة التي تواجهها. لا تنس جميع التوصيات الواردة في القسم السابق.

خطوات إعادة الإنتاج "Steps to Reproduce"

في هذا الحقل، اذكر جميع التعليمات التفصيلية التي تشرح كيفية إثارة المشكلة.

معلومة إضافية "Additional Information"

في هذا القسم، يمكنك تقديم أي معلومات إضافية تعتقد أنها ذات صلة بالمشكلة. إذا كان لديك إصلاح أو حل بديل للمشكلة، فالرجاء تقديمها في هذا القسم.

رفع ملف "Upload File"

لا يمكن تفسير كل شيء بنص عادي. يتيح لك هذا الحقل إرفاق ملفات عشوائية بتقاريرك: لقطات شاشة لإظهار الخطأ، ونماذج المستندات التي تسبب المشكلة، وملفات السجل، وما إلى ذلك.

عرض الحالة "View Status"

اترك هذا الحقل معيناً على "عام" حتى يتمكن الجميع من مشاهدة تقرير الخطأ. استخدم "خاص" فقط للتقارير المتعلقة بالأمان التي تحتوي على معلومات حول الثغرات الأمنية غير المكشوف عنها.

٢.٣.٣.٦. تقديم تقرير خطأ في دبيان

يستخدم دبيان (في الغالب) نظام تتبع الأخطاء المستند إلى البريد الإلكتروني المعروف باسم Debbugs. لفتح تقرير خطأ جديد، سوف ترسل بريدًا إلكترونيًا (مع بنية خاصة) إلى **Submit@bugs.debian.org**. سيؤدي ذلك إلى تخصيص رقم الخطأ XXXXXX وإبلاغك أنه يمكنك إرسال معلومات إضافية عن طريق إرسال **XXXXXX@bugs.debian.org**. يرتبط كل خطأ بحزمة دبيان. يمكنك تصفح جميع أخطاء حزمة معينة (بما في ذلك الخطأ الذي تفكر في الإبلاغ عنه) على **https://bugs.debian.org/package**. يمكنك التحقق من تاريخ خطأ معين على **https://bugs.debian.org/XXXXXX**.

٦.٣.٣.٢.١. إعداد reportbug

بينما يمكنك فتح خطأ جديد باستخدام بريد إلكتروني بسيط، نوصي باستخدام **reportbug** لأنه سيساعدك في صياغة تقرير خطأ قوي يحتوي على جميع المعلومات المطلوبة. من الناحية المثالية، يجب تشغيلها من نظام دبيان (على سبيل المثال، في الجهاز الافتراضي حيث قمت بإعادة إظهار المشكلة).

يبدأ التشغيل الأول لـ `reportbug` برنامجًا نصيًا للتكوين. أولاً، حدد مستوى المهارة. يجب عليك اختيار مبتدئ أو قياسي؛ نستخدم هذا الأخير لأنه يوفر تحكمًا أكثر دقة. بعد ذلك، حدد واجهة وأدخل تفاصيلك الشخصية. أخيرًا، حدد واجهة مستخدم. سيسمح لك البرنامج النصي للتهيئة باستخدام وكيل نقل بريد محلي، أو خادم SMTP، أو كخادم أخير، خادم Debian SMTP.

```
Welcome to reportbug! Since it looks like this is the first time you have

used reportbug, we are configuring its behavior. These settings will be

saved to the file "/root/.reportbugrc", which you will be free to edit

further.

Please choose the default operating mode for reportbug.


1 novice    Offer simple prompts, bypassing technical questions.


2 standard  Offer more extensive prompts, including asking about things
```

that a moderately sophisticated user would be expected to

know about Debian.

3 advanced Like standard, but assumes you know a bit more about Debian,

including "incoming".

4 expert Bypass most handholding measures and preliminary triage

routines. This mode should not be used by people unfamiliar

with Debian's policies and operating procedures.

Select mode: [novice] standard

Please choose the default interface for reportbug.

1 text A text-oriented console user interface

2 gtk2 A graphical (GTK+) user interface.

3 urwid A menu-based console user interface

Select interface: text

Will reportbug often have direct Internet access? (You should answer

yes to this question unless you know what you are doing and plan to

check whether duplicate reports have been filed via some other channel.)

[Y|n|q|?]? Y

What real name should be used for sending bug reports?

[root]> Raphaël Hertzog

Which of your email addresses should be used when sending bug reports?

(Note that this address will be visible in the bug tracking system, so you

may want to use a webmail address or another address with good spam

filtering capabilities.)

[root@localhost.localdomain]> buxy@kali.org

Do you have a "mail transport agent" (MTA) like Exim, Postfix or SSMTP

configured on this computer to send mail to the Internet? [y|N|q|?]? N

Please enter the name of your SMTP host. Usually it's called something

like "mail.example.org" or "smtp.example.org". If you need to use a

different port than default, use the : alternative

format. Just press ENTER if you don't have one or don't know, and so a

Debian SMTP host will be used.

>

Please enter the name of your proxy server. It should only use this

parameter if you are behind a firewall. The PROXY argument should be

formatted as a valid HTTP URL, including (if necessary) a port number; for

example, http://192.168.1.1:3128/. Just press ENTER if you don't have one

or don't know.

>

Default preferences file written. To reconfigure, re-run reportbug with

the "--configure" option.

٢.٢.٣.٣.٦. باستخدام reportbug

بعد اكتمال مرحلة الإعداد، يمكن أن يبدأ تقرير الخطأ الفعلي. ستتم مطالبتك باسم حزمة، على الرغم من أنه يمكنك أيضًا تقديم اسم الحزمة مباشرة على سطر الأوامر بـ **reportbug** *package*).

```
Running 'reportbug' as root is probably insecure! Continue
[y|N|q|?]? y

Please enter the name of the package in which you have
found a problem, or type 'other'

to report a more general problem. If you don't know what
package the bug is in, please

contact debian-user@lists.debian.org for assistance.

> wireshark
```

على عكس النصيحة الواردة أعلاه، إذا كنت لا تعرف أي حزمة بها الخطأ، فيجب عليك الاتصال بمنتدى دعم Kali (الموضح في القسم ٢.٦، "مجتمعات Kali Linux"). في الخطوة التالية، يقوم **reportbug** بتنزيل قائمة الأخطاء التي تم حفظها مقابل الحزمة المحددة ويتيح لك تصفحها لمعرفة ما إذا كان يمكنك العثور عليها.

```
*** Welcome to reportbug.  Use ? for help at prompts. ***

Note: bug reports are publicly archived (including the email address
of

the submitter).

Detected character set: UTF-8

Please change your locale if this is incorrect.

Using '"Raphaël Hertzog" <buxy@kali.org>' as your from address.

Getting status for wireshark...

Verifying package integrity...
```

```
Checking for newer versions at madison...
Will send report to Debian (per lsb_release).
Querying Debian BTS for reports on wireshark (source)...
35 bug reports found:
Bugs with severity important
   1) #478200  tshark: seems to ignore read filters when writing to…
   2) #776206  mergecap: Fails to create output file > 2GB
   3) #780089  wireshark: "On gnome wireshark has not title bar. Does…
Bugs with severity normal
   4) #151017  ethereal: "Protocol Hierarchy Statistics" give misleading…
   5) #275839  doesn't correctly dissect ESMTP pipelining
[...]
  35) #815122  wireshark: add OID 1.3.6.1.4.1.11129.2.4.2
(24-35/35) Is the bug you found listed above [y|N|b|m|r|q|s|f|e|?]? ?
y - Problem already reported; optionally add extra information.
N - (default) Problem not listed above; possibly check more.
b - Open the complete bugs list in a web browser.
m - Get more information about a bug (you can also enter a number
    without selecting "m" first).
r - Redisplay the last bugs shown.
q - I'm bored; quit please.
s - Skip remaining problems; file a new report immediately.
f - Filter bug list using a pattern.
e - Open the report using an e-mail client.
? - Display this help.
(24-35/35) Is the bug you found listed above [y|N|b|m|r|q|s|f|e|?]? n
Maintainer for wireshark is 'Balint Reczey <balint@balintreczey.hu>'.
Looking up dependencies of wireshark...
```

إذا وجدت أن الخطأ الخاص بك قد تم إيداعه بالفعل، فيمكنك اختيار إرسال معلومات تكميلية، وإلا فأنت مدعو لتقديم تقرير خطأ جديد:

```
Briefly describe the problem (max. 100 characters allowed). This will be
the bug email subject, so keep the summary as concise as possible, for
example: "fails to send email" or "does not start with -q option
specified" (enter Ctrl+c to exit reportbug without reporting a bug).
> does not dissect protocol foobar
Rewriting subject to 'wireshark: does not dissect protocol foobar'
```

بعد تقديم ملخص من سطر واحد لمشكلتك، يجب عليك تقييم شدتها على مقياس موسع:

How would you rate the severity of this problem or report?

```
1 critical        makes unrelated software on the system (or the whole
                  system) break, or causes serious data loss, or
                  introduces a security hole on systems where you install
                  the package.
2 grave           makes the package in question unusable by most or all
                  users, or causes data loss, or introduces a security
                  hole allowing access to the accounts of users who use
                  the package.
3 serious         is a severe violation of Debian policy (that is, the
                  problem is a violation of a 'must' or 'required'
                  directive); may or may not affect the usability of the
                  package. Note that non-severe policy violations may be
                  'normal,' 'minor,' or 'wishlist' bugs. (Package
                  maintainers may also designate other bugs as 'serious'
and
                  thus release-critical; however, end users should not do
                  so.). For the canonical list of issues worthing a serious
```

```
                    severity you can refer to this webpage:
                    http://release.debian.org/testing/rc_policy.txt
4 important         a bug which has a major effect on the usability of a
                    package, without rendering it completely unusable to
                    everyone.
5 does-not-build    a bug that stops the package from being built from
source.
                    (This is a 'virtual severity'.)
6 normal            a bug that does not undermine the usability of the whole
                    package; for example, a problem with a particular option
                    or menu item.
7 minor             things like spelling mistakes and other minor cosmetic
                    errors that do not affect the core functionality of the
                    package.
8 wishlist          suggestions and requests for new features.

Please select a severity level: [normal]
```

إذا لم تكن متأكدًا، فما عليك سوى الحفاظ على الخطورة الافتراضية للطبيعي "**normal**".

يمكنك أيضًا وضع علامة على تقريرك ببعض الكلمات الرئيسية:

```
Do any of the following apply to this report?

1 d-i        This bug is relevant to the development of debian-installer.
2 ipv6       This bug affects support for Internet Protocol version 6.
3 l10n       This bug reports a localization/internationalization issue.
4 lfs        This bug affects support for large files (over 2 gigabytes).
5 newcomer   This bug has a known solution but the maintainer requests
someone
             else implement it.
6 patch      You are including a patch to fix this problem.
7 upstream   This bug applies to the upstream part of the package.
8 none
```

```
Please select tags: (one at a time) [none]
```

معظم العلامات ليست مقصورة على فئة معينة، ولكن إذا تضمن تقريرك إصلاحًا، فيجب عليك اختيار علامة **patch**.

بمجرد الانتهاء من ذلك، يفتح **reportbug** محرر نص مع قالب يجب عليك تحريره (مثال ٢.٦. "قالب تم إنشاؤه بواسطة **reportbug**"). يحتوي على بعض الأسئلة التي يجب عليك حذفها والإجابة عليها، بالإضافة إلى بعض المعلومات حول نظامك التي تم جمعها تلقائيًا. لاحظ كيفية بناء الأسطر القليلة الأولى. لا يجب تعديلها حيث سيتم تحليلها بواسطة أداة تتبع الأخطاء لتعيين التقرير إلى الحزمة الصحيحة.

مثال ٢.٦. القالب الذي تم إنشاؤه بواسطة `reportbug`

```
Subject: wireshark: does not dissect protocol foobar

Package: wireshark
Version: 2.0.2+ga16e22e-1
Severity: normal

Dear Maintainer,

*** Reporter, please consider answering these questions,
where appropriate ***

   * What led up to the situation?
   * What exactly did you do (or not do) that was effective
(or
```

ineffective)?

  * What was the outcome of this action?

  * What outcome did you expect instead?

*** End of the template - remove these template lines ***

-- System Information:

Debian Release: stretch/sid

  APT prefers testing

  APT policy: (500, 'testing')

Architecture: amd64 (x86_64)

Foreign Architectures: i386

Kernel: Linux 4.4.0-1-amd64 (SMP w/4 CPU cores)

Locale: LANG=fr_FR.utf8, LC_CTYPE=fr_FR.utf8 (charmap=UTF-8)

Shell: /bin/sh linked to /bin/dash

Init: systemd (via /run/systemd/system)

Versions of packages wireshark depends on:

ii wireshark-qt 2.0.2+ga16e22e-1

wireshark recommends no packages.

wireshark suggests no packages.

-- no debconf information

بمجرد حفظ التقرير وإغلاق محرر النصوص، يمكنك العودة إلى **reportbug**، الذي يوفر العديد من الخيارات والعروض الأخرى لإرسال التقرير الناتج.

```
Spawning sensible-editor...

Report will be sent to "Debian Bug Tracking System" <submit@bugs.debian.org>

Submit this report on wireshark (e to edit) [Y|n|a|c|e|i|l|m|p|q|d|t|s|?]? ?

Y - (default) Submit the bug report via email.

n - Don't submit the bug report; instead, save it in a temporary file (exits reportbug).

a - Attach a file.

c - Change editor and re-edit.

e - Re-edit the bug report.

i - Include a text file.

l - Pipe the message through the pager.

m - Choose a mailer to edit the report.

p - print message to stdout.

q - Save it in a temporary file and quit.

d - Detach an attachment file.

t - Add tags.

s - Add a X-Debbugs-CC recipient (a CC but after BTS processing).

? - Display this help.

Submit this report on wireshark (e to edit) [Y|n|a|c|e|i|l|m|p|q|d|t|s|?]? Y

Saving a backup of the report at /tmp/reportbug-wireshark-backup-20160328-19073-87oJWJ

Connecting to reportbug.debian.org via SMTP...
```

```
Bug report submitted to: "Debian Bug Tracking System" <submit@bugs.debian.org>

Copies will be sent after processing to:

  buxy@kali.org


If you want to provide additional information, please wait to receive the

bug tracking number via email; you may then send any extra information to

n@bugs.debian.org (e.g. 999999@bugs.debian.org), where n is the bug

number. Normally you will receive an acknowledgement via email including

the bug report number within an hour; if you haven't received a

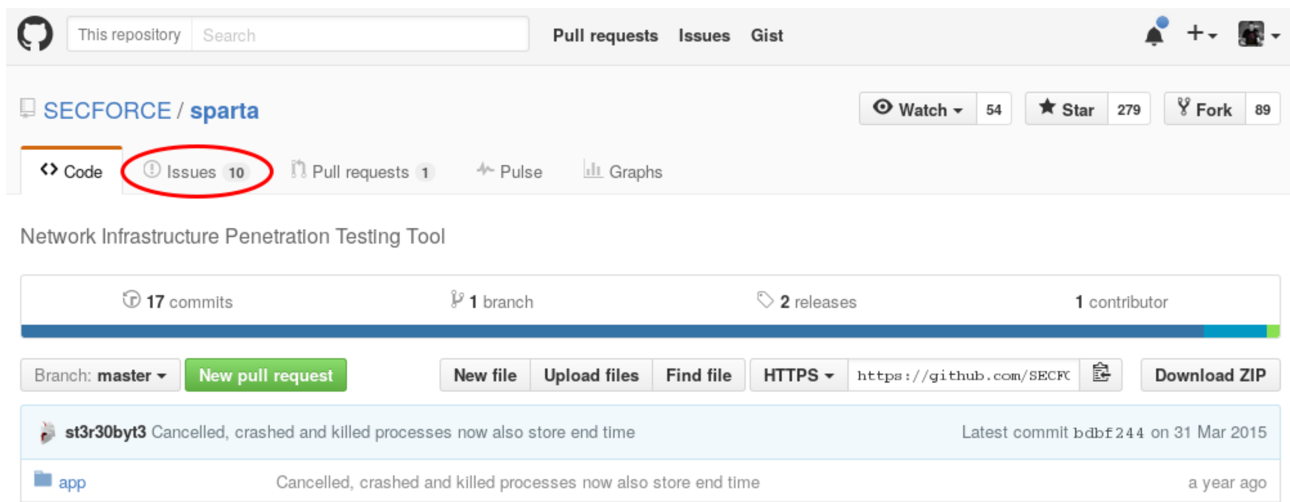
confirmation, then the bug reporting process failed at some point

(reportbug or MTA failure, BTS maintenance, etc.).
```

٣.٣.٣.٦. تقديم تقرير خطأ في مشروع برنامج حر آخر

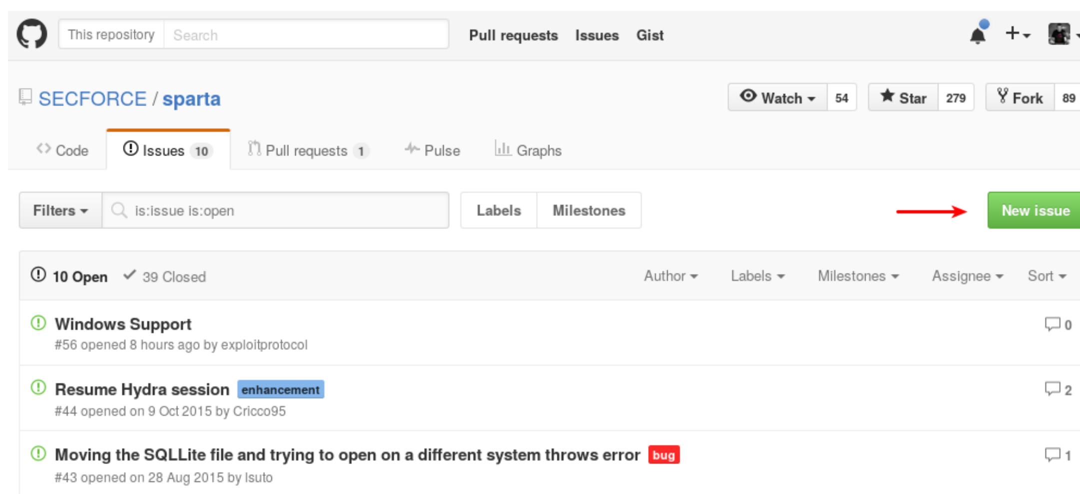
هناك تنوع كبير في مشاريع البرمجيات الحرة، باستخدام سير العمل والأدوات المختلفة. ينطبق هذا التنوع أيضًا على أجهزة تتبع الأخطاء المستخدمة. بينما يتم استضافة العديد من المشاريع على GitHub وتستخدم مشاكل GitHub لتتبع الأخطاء الخاصة بهم، هناك أيضًا العديد من المشاريع الأخرى التي تستضيف برامج التتبع الخاصة بهم، استنادًا إلى Bugzilla و Trac و Redmine و Flyspray وغيرها. معظمها تعتمد على الويب وتتطلب منك تسجيل حساب لإرسال تقرير جديد.

لن نغطي جميع المتعقبات هنا. الأمر متروك لك لمعرفة تفاصيل متتبعات مختلفة لمشاريع برمجيات حرة أخرى، ولكن نظراً لأن GitHub شائع نسبيًا، فسوف نلقي نظرة سريعة عليه هنا. كما هو الحال مع المتعقبات الأخرى، يجب عليك أولاً إنشاء حساب وتسجيل الدخول. بعد ذلك، انقر فوق علامة التبويب المشاكل، كما هو موضح في الشكل ٦.٥، "الصفحة الرئيسية لمشروع GitHub".



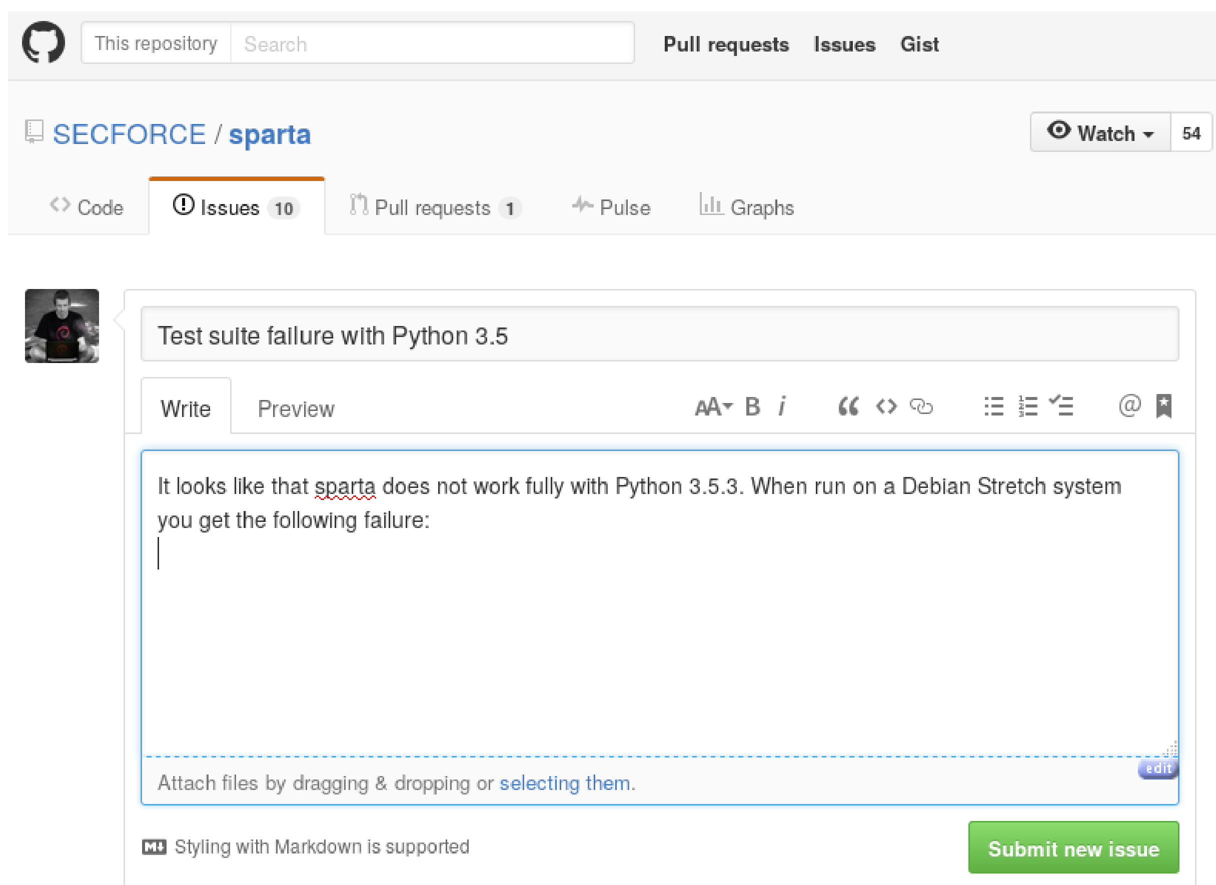
شكل ٦.٥، "الصفحة الرئيسية لمشروع GitHub"

يمكنك بعد ذلك تصفح (والبحث) قائمة المشاكل المفتوحة. بمجرد التأكد من أن الخطأ الخاص بك لم يتم حفظه بعد، يمكنك النقر فوق زر "**New issue**" (الشكل ٦.٦. "صفحة المشاكل الخاصة بمشروع GitHub").



الشكل ٦.٦. صفحة مشكلات مشروع GitHub

أنت الآن في صفحة حيث يجب عليك وصف مشكلتك (الشكل ٧.٦، "نموذج GitHub لتقديم مشكلة جديدة"). على الرغم من عدم وجود قالب مثل النموذج الموجود في reportbug، فإن آلية الإبلاغ عن الأخطاء بسيطة إلى حد ما، مما يسمح لك بإرفاق الملفات وتطبيق التنسيق على النص والمزيد. بالطبع، للحصول على أفضل النتائج، تأكد من اتباع إرشاداتنا لإنشاء تقرير مفصل وموصوف جيدًا.



شكل ٧.٦، "نموذج GitHub لتقديم مشكلة جديدة"

٤.٦ ملخص

ناقشنا في هذا القسم طرقًا مختلفة لمساعدتك في العثور على الوثائق والمعلومات حول البرامج وكيفية العثور على المساعدة بشأن المشكلات التي قد تواجهها. لقد ألقينا نظرة على صفحات **man** و **info** وأوامر **apropos**. ناقشنا أدوات تتبع الأخطاء، وقدمنا بعض النصائح حول كيفية البحث عن تقارير الأخطاء الجيدة وإرسالها، كما قدمنا بعض النصائح لمساعدتك في معرفة من يملك البرنامج أو المشروع المعني.

نصائح تلخيصية:

قبل أن تتمكن من فهم ما يحدث حقًا عند وجود مشكلة، تحتاج إلى معرفة الدور النظري الذي يلعبه كل برنامج مشارك في المشكلة. واحدة من أفضل الطرق للقيام بذلك هي مراجعة وثائق البرنامج.

لعرض صفحة يدوية، ما عليك سوى كتابة **man**، وكتابة اسم الأمر بعد رقم القسم الاختياري.

يعرض الأمر **apropos** قائمة بالصفحات اليدوية التي يذكر ملخصها الكلمات الرئيسية المطلوبة، إلى جانب الملخص المكون من سطر واحد من الصفحة اليدوية.

لقد كتب مشروع GNU أدلة لأغلب برامجه بصيغة المعلومات. هذا هو السبب في أن العديد من الصفحات اليدوية تشير إلى وثائق المعلومات المقابلة.

تحتوي كل حزمة على الوثائق الخاصة بها، وحتى أقل البرامج توثيقًا بشكل عام تحتوي على ملف README يحتوي على بعض المعلومات المهمة. يتم تثبيت هذه الوثائق في المجلد **/usr/share/doc/***package***/**.

في معظم الحالات، قد تعالج الأسئلة الشائعة أو أرشيف القائمة البريدية لموقع الويب الرسمي للبرنامج المشكلات التي واجهتها.

يحتفظ مشروع كالي بمجموعة من الوثائق المفيدة على http://docs.kali.org.

يستخدم مشروع Kali Linux قناة #kali-linux على شبكة Freenode IRC. يمكنك استخدام chat.freenode.net كخادم IRC، على المنفذ 6667 لاتصال مشفر بـ TLS أو المنفذ 6666 لاتصال نص واضح. للانضمام إلى المناقشات حول IRC، يجب عليك استخدام عميل IRC مثل **hexchat** (في الوضع الرسومي) أو **irssi** (في وضع وحدة التحكم). يتوفر أيضًا عميل قائم على الويب على webchat.freenode.net.

توجد منتديات المجتمع الرسمية لمشروع كالي لينكس على forums.kali.org.

إذا كشفت عن خطأ في أحد البرامج، يمكنك البحث في تقارير الأخطاء أو تقديم تقرير خاص بك. تأكد من اتباع الإرشادات التي حددناها للتأكد من أن تقريرك واضح وشامل، ويحسن فرص معالجة المطورين للخطأ في الوقت المناسب.

يجب تقديم بعض تقارير الأخطاء إلى كالي، بينما قد يتم تقديم تقارير أخرى إلى جانب دبيان. أمر مثل `dpkg -s package-name | grep ^Version`: سيكشف عن رقم الإصدار وسيتم وضع علامة عليه باسم "kali" إذا كانت حزمة معدلة من Kali.

عادة ما يكون تحديد مشروع المنبع والعثور على مكان تقديم تقرير الخطأ أمرًا سهلاً. ببساطة تصفح موقع المنبع المشار إليه في حقل Home Page للبيانات الوصفية للتعبئة.

يستخدم Kali أداة تتبع الأخطاء المستندة إلى الويب على https://bugs.kali.org حيث يمكنك استشارة جميع تقارير الأخطاء بشكل مجهول، ولكن إذا كنت ترغب في التعليق أو تقديم تقرير خطأ جديد، فستحتاج إلى تسجيل حساب.

يستخدم دبيان (في الغالب) نظام تتبع الأخطاء المستند إلى البريد الإلكتروني المعروف باسم Debbugs. لفتح تقرير خطأ جديد، يمكنك إرسال بريد إلكتروني (مع بنية خاصة) إلى **Submit@bugs.debian.org** أو يمكنك استخدام الأمر **reportbug**، الذي سيرشدك خلال العملية.

بينما يتم استضافة العديد من المشاريع على GitHub وتستخدم GitHub Issues لتتبع الأخطاء، هناك أيضًا العديد من المشاريع الأخرى التي تستضيف برامج التتبع الخاصة بهم. قد تضطر إلى البحث في أساسيات أجهزة تتبع الأخطاء التابعة لجهات خارجية إذا كنت تريد النشر عليها.

الآن بعد أن حصلت على الأدوات الأساسية للتنقل في Linux، وتثبيت Kali وتكوينه، واستكشاف أخطاء النظام وإصلاحها والحصول على المساعدة، حان الوقت للنظر في قفل Kali حتى تتمكن من حماية التثبيت بالإضافة إلى بيانات العميل.

التمرين الأول للفصل السادس: موارد كالي

١. تريد معرفة ما إذا كان إصدار xyz$ الإصدار الأخير من **nmap** في كالي. ما هو أسرع مورد كالي للتحقق من ذلك؟

٢. ما هما المصدران الأساسيان التفاعليان لدعم مجتمع كالي؟

٣. كيف تبحث في الصفحات اليدوية عن نص معينة؟

الإجابة:

١. لماذا، بالطبع، سيكون ذلك pkg.kali.org، على سبيل المثال، http://pkg.kali.org/nmap.

٢. قناة Kali-Linux IRC# على Freenode ومنتديات Kali.

٣. استخدم الأمر **apropos**.

اختبار الشهادة للفصل السادس

أي أمر سيحدد ما إذا تم تعديل **nmap** بواسطة Kali؟

- **dpkg -l | grep nmap**
- **dpkg -s nmap | grep ^Version**
- **dpkg-query -l | grep nmap**
- جميع ما سبق
- جميع الإجابات خاطئة

ما هو الأمر المستخدم للإبلاغ عن خطأ لمطوري ديان؟

kalibug

bugreport

reportbug

irssi

أي من هذه الإجراءات يمكن استخدامها لإرسال خطأ لمطوري ديان؟

- Use the official Debian bug tracker at https://bugs.debian.org
- Send an email (with a special syntax) to submit@bugs.debian.org
- Use the kalidebug tool directly from Kali Linux and mark the issue as an upstream Debian issue.
- أرسل الخلل إلى متتبع أخطاء Kali الرسمي على https://bugs.kali.org وضع علامة على مشكلة تصحيح دبيان.

الإجابة:

1

- كل ما سبق

2

- **`reportbug`**

3

- Use the official Debian bug tracker at https://bugs.debian.org
- Send an email (with a special syntax) to submit@bugs.debian.org
- Submit the bug to the official Kali bug tracker at https://bugs.kali.org and mark the issue for an upstream Debian patch.

---((الفصل السابع))---

٧. تأمين ومراقبة KALI

عندما تبدأ في استخدام Kali Linux للعمل الذي يزداد حساسية وخصوصية، ستحتاج على الأرجح إلى أخذ أمان التثبيت بجدية أكبر. في هذا الفصل، سنناقش أولاً السياسات الأمنية، مع تسليط الضوء على النقاط المختلفة التي يجب مراعاتها عند تحديد مثل هذه السياسة، وتحديد بعض التهديدات لنظامك ولك بصفتك محترف أمان. سنناقش أيضًا الإجراءات الأمنية لأنظمة الحاسوب المحمول وأجهزة الحاسوب المكتبية ونركز على الجدران النارية وتصفية الحزم. أخيرًا، سنناقش أدوات واستراتيجيات المراقبة ونوضح لك أفضل طريقة لتطبيقها لاكتشاف التهديدات المحتملة لنظامك.

١.٧. تحديد سياسة الأمن

من غير العملي مناقشة الأمن بنقاط ثابتة لأن الفكرة تمثل مجموعة واسعة من المفاهيم والأدوات والإجراءات، والتي لا ينطبق أي منها عالميًا. يتطلب الاختيار من بينها فكرة دقيقة عن أهدافك. يبدأ تأمين النظام بالإجابة على بعض الأسئلة. الاندفاع بتهور نحو تنفيذ مجموعة من الأدوات التعسفية إلى خطر التركيز على الجوانب الخاطئة للأمن.

عادة ما يكون من الأفضل تحديد هدف معين. يبدأ النهج الجيد للمساعدة في هذا التصميم بالأسئلة التالية:

ما الذي تحاول حمايته؟ ستختلف سياسة الأمان اعتمادًا على ما إذا كنت ترغب في حماية أجهزة الحاسوب أو البيانات. في حالة البيانات، تحتاج أيضًا إلى معرفة البيانات.

ما الذي تحاول حمايته؟ هل هو تسرب البيانات السرية؟ فقدان البيانات العرضية؟ خسارة الإيرادات بسبب انقطاع الخدمة؟

أيضا، من الذي تحاول الحماية منه؟ ستكون الإجراءات الأمنية مختلفة تمامًا للحماية من خطأ مطبعي من قبل مستخدم عادي للنظام مقابل الحماية ضد مجموعة مهاجمين من الخارج.

يُستخدم مصطلح "الخطر "risk"" عادة للإشارة بشكل عام لهذه العوامل الثلاثة:

ما الذي يجب حمايته، وما الذي يجب منعه، ومن الذي قد يحدث ذلك.

تتطلب نمذجة المخاطر إجابات على هذه الأسئلة الثلاثة. من نموذج المخاطر هذا، يمكن بناء سياسة أمنية وتنفيذ السياسة بإجراءات ملموسة.

تحقق دائما

يحاول بروس شناير، الخبير العالمي في شؤون الأمن (ليس فقط أمن الحاسوب)، مواجهة واحدة من أهم خرافات الأمن بشعار: "الأمن عملية وليس منتجًا". تتغير الموارد المطلوب حمايتها بمرور الوقت وكذلك تتغير التهديدات والوسائل المتاحة للمهاجمين. حتى لو تم تصميم وتنفيذ سياسة أمنية بشكل مثالي في البداية، يجب ألا ترتاح أبداً. تتطور مكونات الخطر ويجب أن تتطور الاستجابة لذلك الخطر وفقًا لذلك.

تستحق القيود الإضافية أيضًا أن تؤخذ في الاعتبار، لأنها يمكن أن تحد من نطاق السياسات المتاحة. إلى أي مدى أنت على استعداد لتأمين النظام؟ هذا السؤال له تأثير كبير على السياسة التي يتعين تنفيذها. في كثير من الأحيان، يتم تحديد الإجابة فقط من حيث التكاليف النقدية، ولكن يجب أيضًا مراعاة عناصر أخرى، مثل مقدار الإزعاج المفروض على مستخدمي النظام أو تدهور الأداء.

بمجرد نمذجة الخطر، يمكنك البدء في التفكير في تصميم سياسة أمنية حقيقية.

هناك حالات شاذة يمكن أن تلعب دورها عند تحديد مستوى الحماية الأمنية التي يجب اعتمادها. من ناحية، يمكن أن يكون من السهل للغاية توفير أمان النظام الأساسي.

على سبيل المثال، إذا كان النظام المراد حمايته يتألف فقط من حاسوب مستعمل، يكون استخدامه الوحيد هو إضافة عدد قليل من الأرقام في نهاية اليوم، فإن اتخاذ قرار بعدم القيام بأي شيء خاص لحمايته سيكون أمرًا معقولًا تمامًا. القيمة الجوهرية للنظام منخفضة وقيمة البيانات صفر حيث لا يتم تخزينها على الحاسوب. المهاجم المحتمل التسلل إلى هذا النظام سيحصل على آلة حاسبة فقط. من المحتمل أن تكون تكلفة تأمين مثل هذا النظام أكبر من تكلفة الخرق.

في الطرف الآخر من النطاق، قد ترغب في حماية سرية البيانات السرية بأكثر طريقة شاملة ممكنة، متفوقة على أي اعتبار آخر. في هذه الحالة، سيكون الرد المناسب هو التدمير الكامل للبيانات (محو الملفات بشكل آمن، وتمزيق الأقراص الصلبة إلى أجزاء، ثم إذابة هذه الأجزاء في الحمض، وما إلى ذلك). إذا كان هناك مطلب إضافي بوجوب حفظ البيانات في المخزن للاستخدام المستقبلي (على الرغم من عدم توفرها بسهولة بالضرورة)، وإذا لم تكن التكلفة عاملاً، فستكون نقطة البداية هي تخزين البيانات على لوحات سبائك إيريديوم - بلاتينيوم المخزنة في مخابئ واقية من القنابل تحت جبال مختلفة في العالم، كل منها (بالطبع) سرية تمامًا وتحرسها جيوش بأكملها.

على الرغم من أن هذه الأمثلة قد تبدو شاذة، إلا أنها قد تكون استجابة كافية لبعض المخاطر المحددة، بقدر ما هي نتيجة عملية فكرية تأخذ في الاعتبار الأهداف التي يجب الوصول إليها والقيود التي يجب تحقيقها. عند اتخاذ قرار منطقي، لا توجد سياسة أمنية محترمة أكثر أو أقل من أي سياسة أخرى.

بالعودة إلى حالة أكثر نموذجية، يمكن تقسيم نظام المعلومات إلى أنظمة فرعية متسقة ومعظمها مستقلة. سيكون لكل نظام فرعي متطلباته وقيوده الخاصة، وبالتالي يجب إجراء تقييم المخاطر وتصميم السياسة الأمنية بشكل منفصل لكل منهما. من المبادئ الجيدة التي يجب وضعها في الاعتبار أن سطح الهجوم الصغير أسهل في الدفاع عنه من السطح الكبير. يجب أيضًا أن يتم تصميم تنظيم الشبكة وفقًا لذلك: يجب أن تركز الخدمات الحساسة على عدد صغير من الأجهزة، ويجب ألا يمكن الوصول إلى هذه الأجهزة إلا من خلال الحد الأدنى من المسارات أو نقاط التفتيش. المنطق واضح: من الأسهل تأمين نقاط التفتيش هذه من تأمين جميع الآلات الحساسة ضد العالم الخارجي بأكمله. عند هذه النقطة تظهر فائدة تصفية الشبكة (بما في ذلك جدران الحماية). يمكن تنفيذ هذا التصفية باستخدام أجهزة مخصصة ولكن الحل الأبسط والأكثر مرونة هو استخدام برنامج جدار حماية مثل ذلك الذي تم دمجه في نواة Linux.

٢.٧. التدابير الأمنية الممكنة

كما أوضح الباب السابق، لا يوجد رد واحد على السؤال حول كيفية تأمين Kali Linux. كل هذا يتوقف على كيفية استخدامه وما تحاول حمايته.

١.٢.٧. على الخادم

إذا قمت بتشغيل Kali Linux على خادم يمكن الوصول إليه بشكل عام، فأنت على الأرجح ترغب في تأمين خدمات الشبكة عن طريق تغيير أي كلمات مرور افتراضية يمكن تكوينها (انظر القسم ٣.٧، "تأمين خدمات الشبكة") وربما أيضًا عن طريق تقييد وصولهم بجدار حماية (راجع القسم ٤.٧، "جدار الحماية أو تصفية الحزم").

إذا قمت بتوزيع حسابات المستخدمين إما مباشرة على الخادم أو على إحدى الخدمات، فأنت تريد التأكد من تعيين كلمات مرور قوية (يجب أن تقاوم هجمات القوة الغاشمة). في الوقت نفسه، قد ترغب في إعداد *fail2ban*، الذي سيجعل الأمر أكثر صعوبة هجمات القوة الغاشمة عبر الشبكة (من خلال تصفية عناوين IP التي تتجاوز حد محاولات تسجيل الدخول الفاشلة). قم بتثبيت *fail2ban* بـ **apt update** يليه **apt install fail2ban**.

إذا قمت بتشغيل خدمات الويب، فربما تريد استضافتها عبر HTTPS لمنع وسطاء الشبكة من استنشاق حركة المرور الخاصة بك (والتي قد تتضمن ملفات تعريف ارتباط المصادقة).

٢.٢.٧. على جهاز حاسوب محمول

لا يخضع الحاسوب المحمول الخاص بأداة اختبار الاختراق لنفس المخاطر التي يتعرض لها الخادم العام: على سبيل المثال، يقل احتمال تعرضك لعمليات مسح عشوائية من أطفال البرامج النصية وحتى عندما تكون كذلك، فربما لن يكون لديك أي خدمات شبكة ممكّنة.

غالبًا ما تنشأ المخاطر الحقيقية عند السفر من عميل إلى آخر. على سبيل المثال، يمكن سرقة الحاسوب المحمول أثناء السفر أو الاستيلاء عليه من قبل الجمارك. هذا هو السبب في أنك على الأرجح ترغب في استخدام تشفير كامل للقرص (انظر القسم ٢.٢.٤، "التثبيت على نظام ملفات مشفر بالكامل") وربما أيضًا إعداد ميزة "nuke": البيانات التي جمعتها أثناء ارتباطاتك سرية وتتطلب أقصى درجات الحماية.

قد تحتاج أيضًا إلى قواعد جدار الحماية (انظر القسم ٤.٧، "جدار الحماية أو تصفية الحزم") ولكن ليس للغرض نفسه كما في الخادم. قد ترغب في منع كل حركة المرور الصادرة باستثناء حركة المرور الناتجة عن وصول VPN الخاص بك. يُقصد بهذا كشبكة أمان، بحيث عندما تعطل الشبكة الافتراضية الخاصة، تلاحظها على الفور (بدلاً من العودة إلى الوصول إلى الشبكة المحلية). وبهذه الطريقة، لا تفشي عناوين IP الخاصة بعملائك عند تصفح الويب أو القيام بأنشطة أخرى عبر الإنترنت. بالإضافة إلى ذلك، إذا كنت تؤدي مشاركة داخلية محلية، فمن الأفضل أن تظل متحكمًا في جميع أنشطتك لتقليل الضوضاء التي تحدثها على الشبكة، والتي يمكن أن تنبه العميل وأنظمة الدفاع الخاصة به.

٣.٧. تأمين خدمات الشبكة

بشكل عام، يعد تعطيل الخدمات التي لا تستخدمها فكرة جيدة. يسهّل Kali القيام بذلك نظراً لأن معظم خدمات الشبكة معطلة افتراضياً.

طالما أن الخدمات لا تزال معطلة، فإنها لا تشكل أي تهديد أمني. ومع ذلك، يجب أن تكون حذرًا عند تمكينها للأسباب التالية:

١. لا يوجد جدار حماية افتراضياً، لذلك إذا استمعوا إلى جميع واجهات الشبكة، فستكون متاحة للجمهور بشكل نشط.
٢. لا تحتوي بعض الخدمات على بيانات اعتماد المصادقة وتتيح لك تعيينها عند الاستخدام الأول؛ الآخرون لديهم بيانات اعتماد افتراضية (وبالتالي معروفة على نطاق واسع). تأكد من (إعادة) تعيين أي كلمة مرور لشيء تعرفه أنت فقط.
٣. تعمل العديد من الخدمات كجذر مع امتيازات المسؤول الكاملة، وبالتالي فإن عواقب الوصول غير المصرح به أو خرق الأمان عادة ما تكون شديدة.

الشهادات الإفتراضية

لن نذكر هنا جميع الأدوات التي تأتي مع الشهادات الافتراضية، بدلاً من ذلك يجب عليك التحقق من ملف README.Debian للحزم المعنية، وكذلك docs.kali.org و tools.kali.org لمعرفة ما إذا كانت الخدمة تحتاج إلى بعض الميزات الخاصة الحرص على تأمينها.

إذا كنت تعمل في الوضع المباشر، فإن كلمة مرور الحساب الجذر هي "toor". وبالتالي، يجب ألا تقوم بتمكين SSH قبل تغيير كلمة المرور للحساب الجذر، أو قبل أن تعدل تكوينها لعدم السماح بتسجيلات الدخول المستندة إلى كلمة المرور.

لاحظ أيضًا أن مشروع BeEF (من الحزمة المثبتة بالفعل beef-xss) معروف أيضا بامتلاكه لبيانات الاعتماد الافتراضية "beef" ، كلمة المرور "beef") في ملف التكوين الافتراضي الخاص به.

4.7. جدار الحماية أو تصفية الحزم

جدار الحماية هو قطعة من أجهزة الحاسوب التي تحتوي على أجهزة أو برامج أو كليهما يوزع حزم الشبكة الواردة أو الصادرة (القادمة من شبكة محلية أو المغادرة منها) ويسمح فقط من خلال تلك المطابقة لشروط معينة محددة مسبقًا.

بوابة شبكة التصفية هي نوع من جدار الحماية الذي يحمي شبكة كاملة. عادة ما يتم تثبيته على جهاز مخصص تم تكوينه كبوابة للشبكة بحيث يمكنه تحليل جميع الحزم التي تمر من وإلى الشبكة. بدلاً من ذلك، يعد جدار الحماية المحلي خدمة برمجية يتم تشغيلها على جهاز معين من أجل تصفية أو تقييد الوصول إلى بعض الخدمات على هذا الجهاز، أو ربما لمنع الاتصالات الصادرة عن طريق برنامج خبيث يمكن للمستخدم تثبيته، سواء عن قصد أو بدونه.

تشتمل نواة Linux على جدار الحماية *netfilter*. لا يوجد حل جاهز لتكوين أي جدار حماية نظراً لاختلاف متطلبات الشبكة والمستخدم. ومع ذلك، يمكنك التحكم في netfilter من مساحة المستخدم باستخدام أوامر **iptables** و **ip6tables**. الفرق بين هذين الأمرين هو أن الأول يعمل لشبكات IPv4، بينما يعمل الأخير على IPv6؛ نظراً لأن مكدسي بروتوكولات الشبكة قد يكونان متاحين لسنوات عديدة، فستحتاج كلتا الأداتين إلى الاستخدام بالتوازي. يمكنك أيضًا استخدام أداة **fwbuilder** الممتازة المستندة إلى واجهة المستخدم الرسومية، والتي توفر تمثيلاً رسومياً لقواعد التصفية.

ومع ذلك، قررت تكوينه، netfilter هو تطبيق جدار حماية Linux، لذلك دعونا نلقي نظرة فاحصة على كيفية عمله.

١.٤.٧. سلوك Netfilter

تستخدم Netfilter أربعة جداول مميزة، تخزن القواعد التي تنظم ثلاثة أنواع من العمليات على الحزم:

filter: يتعلق بقواعد التصفية (قبول الحزمة أو رفضها أو تجاهلها).

nat: (ترجمة عنوان الشبكة "Network Address Translation") تتعلق بترجمة عناوين المصدر أو الوجهة ومنافذ الحزم.

mangle: يتعلق بتغييرات أخرى لحزم IP (بما في ذلك ToS - نوع الخدمة - الحقل والخيارات).

raw: يسمح بتعديلات يدوية أخرى على الحزم قبل وصولها إلى نظام تتبع الاتصال.

يحتوي كل جدول على قوائم قواعد تسمى *السلاسل "chains"*. يستخدم جدار الحماية سلاسل قياسية للتعامل مع الحزم بناءً على ظروف محددة مسبقًا. يمكن للمسؤول إنشاء سلاسل أخرى، والتي سيتم استخدامها فقط عند الإشارة إليها بواسطة إحدى السلاسل القياسية (سواء بشكل مباشر أو غير مباشر).

يحتوي جدول filter على ثلاث سلاسل قياسية:

INPUT: يتعلق بالحزم التي يكون وجهتها الجدار الناري نفسه.

OUTPUT: يتعلق بالحزم المنبعثة من جدار الحماية.

FORWARD: تتعلق الحزم التي تمر عبر جدار الحماية (وهو ليس مصدرها ولا وجهتها).

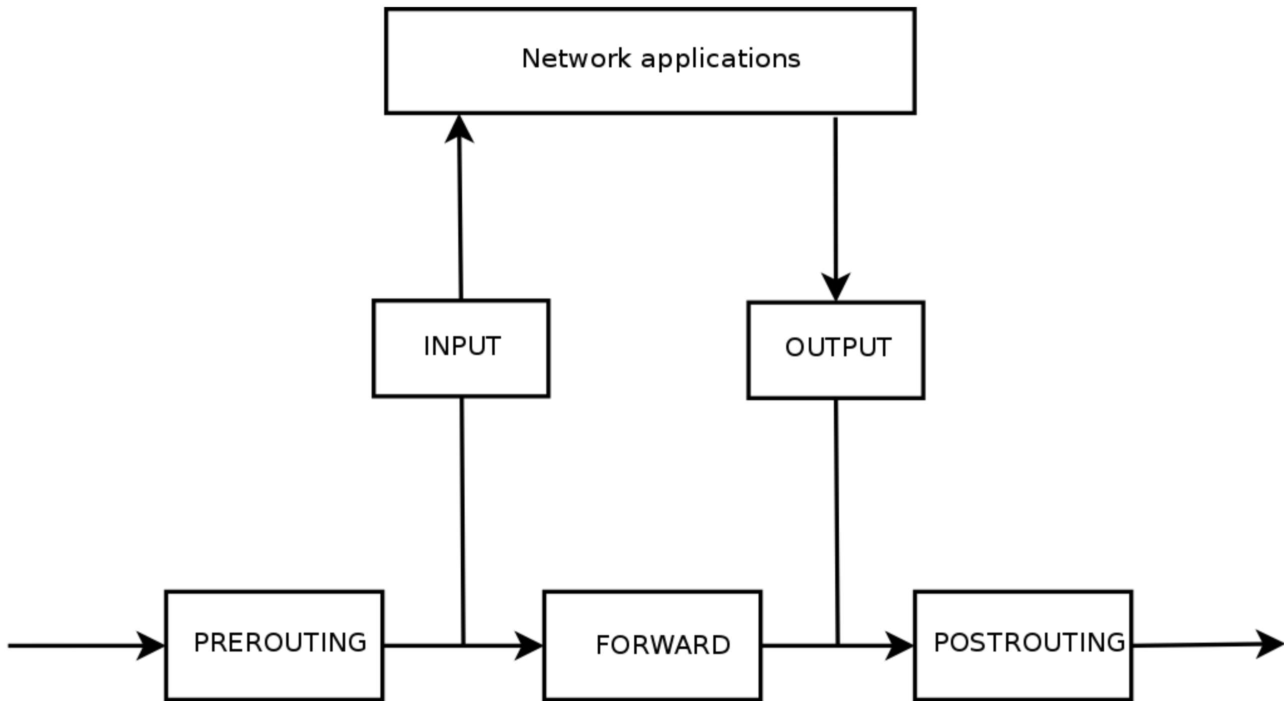
يحتوي جدول nat أيضًا على ثلاث سلاسل قياسية:

PREROUTING: تعديل الحزم بمجرد وصولها.

POSTROUTING: تعديل الحزم عندما تكون جاهزة للذهاب في طريقها.

OUTPUT (الإخراج): لتعديل الحزم التي تم إنشاؤها بواسطة جدار الحماية نفسه.

يتم توضيح هذه السلاسل في الشكل ١.٧، "كيف يتم استدعاء سلاسل Netfilter".



الشكل ١.٧. كيف يتم استدعاء سلاسل Netfilter

كل سلسلة قائمة بالقواعد. كل قاعدة هي مجموعة من الشروط وإجراء للقيام به عند استيفاء الشروط. عند معالجة حزمة، يقوم جدار الحماية بمسح السلسلة المناسبة، وقاعدة تلو الأخرى، وعندما يتم استيفاء الشروط لقاعدة واحدة، فإنه يقفز (ومن ثم يكون الخيار j- في الأوامر) إلى

الإجراء المحدد لمتابعة المعالجة. السلوكيات الأكثر شيوعًا هي إجراءات موحدة ومخصصة لهم. يؤدي اتخاذ أحد هذه الإجراءات القياسية إلى مقاطعة معالجة السلسلة، لأن مصير الحزم مختوم بالفعل (باستثناء الاستثناء المذكور أدناه). فيما يلي إجراءات Netfilter.

ACCEPT: السماح للحزمة في طريقها.

REJECT: رفض الحزمة باستخدام حزمة خطأ بروتوكول رسائل التحكم في الإنترنت (ICMP) (يحدد خيار reject-with type-- من iptables نوع الخطأ الذي سيتم إرساله).

DROP: حذف (تجاهل) الحزمة.

LOG: تسجيل (عبر syslogd) رسالة مع وصف الحزمة. لاحظ أن هذا الإجراء لا يقاطع العملية، ويستمر تنفيذ السلسلة في القاعدة التالية، وهذا هو السبب في أن تسجيل الحزم المرفوضة يتطلب كلاً من LOG وقاعدة REJECT / DROP. تشمل المعلمات الشائعة المرتبطة بالتسجيل ما يلي:

log-level--، مع القيمة الافتراضية تحذير "warning"، يشير إلى مستوى خطورة سجل النظام.

يسمح **log-prefix**-- بتحديد بادئة نصية للتمييز بين الرسائل المسجلة.

يشير كل من **log-tcp-sequence**-- و **log-tcp-options**-- و **log-ip-options**-- إلى بيانات إضافية يتم دمجها في الرسالة: على التوالي رقم تسلسل TCP وخيارات TCP وخيارات IP.

ULOG: تسجيل رسالة عبر ulogd، والتي يمكن تكييفها بشكل أفضل وأكثر كفاءة من syslogd للتعامل مع أعداد كبيرة من الرسائل؛ لاحظ أن هذا الإجراء، مثل LOG، يعيد أيضًا المعالجة إلى القاعدة التالية في سلسلة الاستدعاء.

chain_name: القفز إلى السلسلة المعينة وتقييم قواعدها.

RETURN: مقاطعة عملية السلسلة الحالية والعودة إلى سلسلة الاستدعاء؛ في حالة أن السلسلة الحالية هي سلسلة قياسية، لا توجد سلسلة اتصال، لذلك يتم تنفيذ الإجراء الافتراضي (المحدد بخيار P- إلى iptables) بدلاً من ذلك.

SNAT (فقط في جدول **nat**): تطبيق ترجمة عنوان شبكة المصدر (SNAT). تصف الخيارات الإضافية التغييرات الدقيقة لتطبيقها، بما في ذلك خيار to-source address: port--، الذي يحدد عنوان IP المصدر الجديد و / أو المنفذ.

DNAT (فقط في جدول **nat**): تطبيق ترجمة عنوان شبكة الوجهة (DNAT). تصف الخيارات الإضافية التغييرات الدقيقة لتطبيقها، بما في ذلك خيار *address:port* to-destination--، الذي يحدد عنوان IP الجديد للوجهة و / أو المنفذ.

MASQUERADE (فقط في جدول **nat**): تطبيق التنكر "masquerading " (حالة خاصة من Source NAT).

REDIRECT (فقط في جدول **nat**): إعادة توجيه حزمة بشفافية إلى منفذ معين من جدار الحماية نفسه؛ يمكن استخدام هذا لإعداد وكيل ويب شفاف يعمل بدون تكوين على جانب العميل، حيث يعتقد العميل أنه يتصل بالمستلم بينما تمر الاتصالات فعلياً عبر الوكيل. يشير خيار *port(s)* **to-ports**--إلى المنفذ، أو نطاق المنفذ، حيث يجب إعادة توجيه الحزم.

الإجراءات الأخرى، وخاصة تلك المتعلقة بالجدول **mangle**، تقع خارج نطاق هذا النص. تحتوي صفحات iptables(8) و (8) ip6tables على قائمة شاملة.

ما هو ICMP؟

بروتوكول رسائل التحكم في الإنترنت (ICMP) هو البروتوكول المستخدم لإرسال المعلومات الإضافية عن الاتصالات. يختبر اتصال الشبكة باستخدام الأمر **ping**، الذي يرسل رسالة طلب صدى "ICMP "echo request، والتي من المفترض أن يجيب عليها المستلم برسالة رد صدى "ICMP "echo reply. يشير إلى جدار حماية يرفض حزمة، ويشير إلى تجاوز سعة في المخزن المؤقت للاستلام، ويقترح مسارًا أفضل للحزم التالية في الاتصال، وما إلى ذلك. يتم تعريف هذا البروتوكول من خلال العديد من وثائق RFC. كان RFC777 و RFC792 الأول، ولكن العديد من الآخرين وسعوا و/أو راجعوا البروتوكول.

http://www.faqs.org/rfcs/rfc777.html

http://www.faqs.org/rfcs/rfc792.html

كمرجع، يعد المخزن المؤقت للاستلام منطقة ذاكرة صغيرة تخزن البيانات بين الوقت الذي تصل فيه من الشبكة والوقت الذي تعالجه فيه النواة. إذا كانت هذه المنطقة ممتلئة، فلا يمكن تلقي بيانات جديدة وتشير ICMP إلى المشكلة بحيث يمكن للمرسل إبطاء معدل النقل (الذي يجب أن يصل إلى التوازن بشكل مثالي بعد مرور بعض الوقت).

لاحظ أنه على الرغم من أن شبكة IPv4 يمكن أن تعمل بدون ICMP، إلا أن ICMPv6 مطلوب بشدة لشبكة IPv6، نظرًا لأنه يجمع بين العديد من الوظائف التي انتشرت في عالم IPv4 عبر ICMPv4 وبروتوكول عضوية مجموعة الإنترنت " Internet Group Membership Protocol" (IGMP) وبروتوكول تحليل العنوان (ARP).

تم تعريف ICMPv6 في RFC4443.

http://www.faqs.org/rfcs/rfc4443.html

٢.٤.٧. بناء الجملة من iptables و ip6tables

يتم استخدام أوامر **iptables** و **ip6tables** لمعالجة الجداول والسلاسل والقواعد. يشير خيار **t table-** الخاص بهم إلى الجدول الذي سيعمل عليه (بشكل افتراضي، **filter**).

١.٢.٤.٧. أوامر

الخيارات الرئيسية للتفاعل مع السلاسل:

chain **L-** : يسرد القواعد في السلسلة. يُستخدم هذا عادةً مع الخيار **n-** لتعطيل تحليل الاسم (على سبيل المثال، **iptables -n -L INPUT** سيعرض القواعد المتعلقة بالحزم الواردة).

chain **N-** : ينشئ سلسلة جديدة. يمكنك إنشاء سلاسل جديدة لعدد من الأغراض، بما في ذلك اختبار خدمة شبكة جديدة أو صد هجوم على الشبكة.

chain **X-** : تحذف سلسلة فارغة وغير مستخدمة (على سبيل المثال، iptables -X ddos-attack).

chain rule **A-** : يضيف قاعدة في نهاية السلسلة المعطاة. تذكر أن القواعد تتم معالجتها من الأعلى إلى الأسفل، لذا تأكد من مراعاة ذلك عند إضافة القواعد.

chain rule_num rule **I-** : يدرج قاعدة قبل القاعدة رقم Rule_num. كما هو الحال مع الخيار **A-** ، ضع أمر المعالجة في الاعتبار عند إدراج قواعد جديدة في سلسلة.

-D *chain rule_num* (or **-D** *chain rule*): تحذف قاعدة في سلسلة؛ تحدد الصيغة الأولى القاعدة التي سيتم حذفها من خلال رقمها (**iptables -L --line-numbers** ستعرض أرقام الأسطر)، بينما يحددها الأخير من خلال محتوياته.

-F *chain* : مسح سلسلة (حذف كافة قواعدها). على سبيل المثال، لحذف جميع القواعد المتعلقة بالحزم الصادرة، يمكنك تشغيل `iptables -F OUTPUT`. إذا لم يتم ذكر سلسلة، يتم حذف جميع القواعد في الجدول.

-P *chain action* يحدد الإجراء الافتراضي، أو "السياسة" لسلسلة معينة؛ لاحظ أن السلاسل القياسية فقط يمكن أن يكون لها مثل هذه السياسة. لإسقاط كل حركة المرور الواردة بشكل افتراضي، ستقوم بتشغيل `iptables -P INPUT DROP`.

٢.٢.٤.٧. قواعد

يتم التعبير عن كل قاعدة كـ *conditions* **-j** *action action_options*. إذا تم وصف العديد من الشروط في نفس القاعدة، فإن المعيار هو اقتران (logical *AND*) الشروط، والتي تكون على الأقل مقيدة مثل كل حالة على حدة.

يطابق شرط **-p** *protocol* مجال بروتوكول حزمة IP. القيم الأكثر شيوعًا هي tcp و udp و icmp و icmpv6. يمكن استكمال هذا الشرط بشروط على منافذ TCP، مع عبارات مثل: **--source-port** *port* و **--destination-port** *port*.

شروط سلبية

يؤدي إجراء شرط مسبق بعلامة تعجب إلى إبطال الشرط. على سبيل المثال: يتعارض رفض شرط في الخيار p- مع "أي حزمة ببروتوكول مختلف عن البروتوكول المحدد". يمكن تطبيق آلية النفي هذه على جميع الشروط الأخرى أيضًا.

يتطابق شرط **s** *address*- أو **s** *network/mask*- مع عنوان مصدر الحزمة. بالمقابل، فإن **d** *address* - أو **d** *network/mask*- يطابق عنوان الوجهة.

يختار شرط **i** *interface*- الحزم القادمة من واجهة الشبكة المحددة. **o** *interface*- تختار الحزم التي تخرج على واجهة معينة.

يطابق شرط **state** *state*-- حالة الحزمة في اتصال (وهذا يتطلب وحدة **ipt_conntrack** النواة لتتبع الاتصال). تصف الحالة **NEW** حزمة تبدأ اتصالًا جديدًا، وتتطابق **ESTABLISHED** مع الحزم التي تنتمي إلى اتصال موجود بالفعل، وتتطابق **RELATED** مع الحزم التي تبدأ اتصالًا جديدًا متعلقًا باتصال موجود (وهو أمر مفيد لاتصالات **ftp-data** في الوضع "النشط") بروتوكول FTP).

هناك العديد من الخيارات المتاحة ل **iptables** و **ip6tables** وإتقانها كلها تتطلب قدرا كبيرا من الدراسة والخبرة. ومع ذلك، فإن أحد الخيارات التي ستستخدمها في الغالب هو

حظر حركة مرور الشبكة الضارة من مضيف أو مجموعة من المضيفين. على سبيل المثال، لحظر حركة المرور الواردة بصمت من عنوان ip 10.0.1.5 والشبكة الفرعية من الفئة C :31.13.74.0/24

```
# iptables -A INPUT -s 10.0.1.5 -j DROP
# iptables -A INPUT -s 31.13.74.0/24 -j DROP
# iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.1.5             0.0.0.0/0
DROP       all  --  31.13.74.0/24        0.0.0.0/0
```

أمر **iptables** آخر شائع الاستخدام هو السماح بحركة مرور الشبكة لخدمة أو منفذ معين. للسماح للمستخدمين بالاتصال بـ SSH و HTTP و IMAP، يمكنك تشغيل الأوامر التالية:

```
# iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
# iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
# iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT
# iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.1.5             0.0.0.0/0
DROP       all  --  31.13.74.0/24        0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
```

تعتبر النظافة الجيدة للحاسوب لتنظيف القواعد القديمة وغير الضرورية. أسهل طريقة لحذف قواعد **iptables** هي الرجوع إلى القواعد حسب رقم السطر، والتي يمكنك استرجاعها باستخدام خيار **line-numbers--**. كن حذرًا على الرغم من ذلك: سيؤدي إسقاط قاعدة إلى إعادة ترقيم جميع القواعد التي تظهر بشكل أكبر في السلسلة.

```
# iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  10.0.1.5             0.0.0.0/0
2    DROP       all  --  31.13.74.0/24        0.0.0.0/0
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
# iptables -D INPUT 2
# iptables -D INPUT 1
# iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
2    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
```

هناك شروط أكثر تحديدًا، اعتمادًا على الشروط العامة الموضحة أعلاه. لمزيد من المعلومات، راجع (8) iptables و (8) ip6tables.

٣.٤.٧. إنشاء قواعد

تتطلب كل عملية إنشاء قاعدة استدعاء **iptables** أو **ip6tables**. قد تكون كتابة هذه الأوامر يدويًا مملة، لذلك يتم تخزين المكالمات عادة في برنامج نصي بحيث يتم تكوين النظام تلقائيًا بنفس الطريقة في كل مرة يتم فيها تشغيل الجهاز. يمكن كتابة هذا البرنامج النصي يدويًا ولكن قد يكون من المفيد أيضًا إعداده باستخدام أداة عالية المستوى مثل **fwbuilder**.

```
# apt install fwbuilder
```

المبدأ بسيط. في الخطوة الأولى، صف جميع العناصر التي ستشارك في القواعد الفعلية:

جدار الحماية نفسه، مع واجهات شبكته

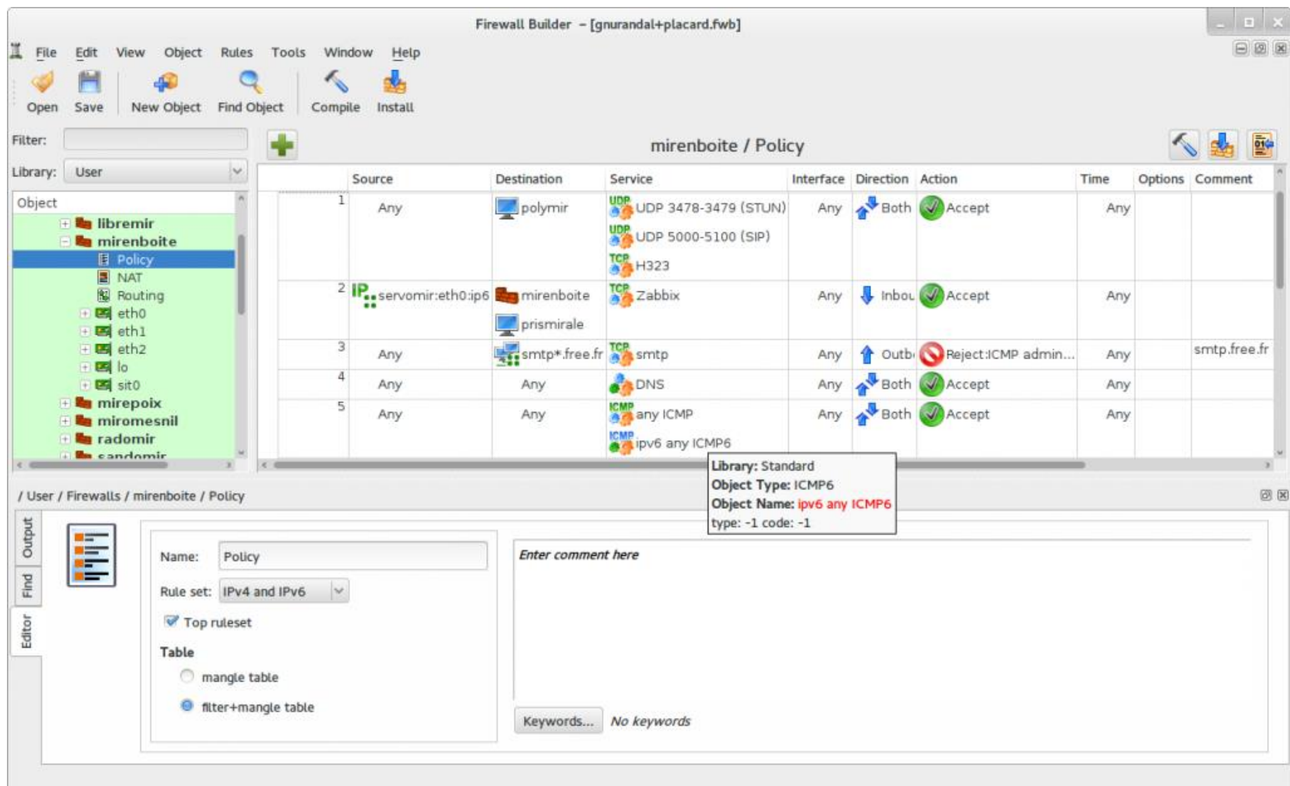
الشبكات بنطاقات IP المقابلة لها

الخوادم

المنافذ التابعة للخدمات المستضافة على الخوادم

بعد ذلك، قم بإنشاء القواعد بإجراءات السحب والإفلات البسيطة على الكائنات كما هو موضح في الشكل ٢.٧، "النافذة الرئيسية لـ Fwbuilder". يمكن لبعض القوائم السياقية تغيير الحالة (نفيها، على سبيل المثال). ثم يجب اختيار الإجراء وتكوينه.

بقدر ما يتعلق الأمر بـ IPv6، يمكنك إما إنشاء مجموعتي قواعد مميزتين لـ IPv4 و IPv6، أو إنشاء واحدة فقط والسماح لـ **fwbuilder** بترجمة القواعد وفقًا للعناوين المخصصة للكائنات.



شكل ٢.٧، "النافذة الرئيسية لـ Fwbuilder"

سيقوم **fwbuilder** بإنشاء برنامج نصي يقوم بتكوين جدار الحماية وفقًا للقواعد التي حددتها. تمنحه بنيتها المعيارية القدرة على إنشاء برامج نصية تستهدف أنظمة مختلفة بما في ذلك **`iptables`** لنظام Linux و **`ipf`** لـ FreeBSD و **`pf`** لـ OpenBSD.

٤.٤.٧. تثبيت القواعد في كل إقلاع

من أجل تنفيذ قواعد جدار الحماية في كل مرة يتم فيها تشغيل الجهاز، ستحتاج إلى تسجيل البرنامج النصي للتكوين في توجيه **up** لملف **/etc/network/interfaces**. في المثال التالي، يتم تخزين البرنامج النصي في **/usr/local/etc/arrakis.fw**.

```
auto eth0
iface eth0 inet static
    address 192.168.0.1
    network 192.168.0.0
    netmask 255.255.255.0
    broadcast 192.168.0.255
    up /usr/local/etc/arrakis.fw
```

يفترض هذا المثال أنك تستخدم **ifupdown** لتكوين واجهات الشبكة. إذا كنت تستخدم شيئًا آخر (مثل NetworkManager أو systemd-networkd)، فارجع إلى الوثائق الخاصة بها لمعرفة طرق تنفيذ برنامج نصي بعد طرح الواجهة.

٥.٧. المراقبة والتسجيل

تعد سرية البيانات وحمايتها جانبًا مهمًا من جوانب الأمن، ولكن من المهم بنفس القدر ضمان توفر الخدمات. بصفتك مشرفًا وممارسًا للأمان، يجب عليك التأكد من أن كل شيء يعمل كما هو متوقع، وتقع على عاتقك مسؤولية اكتشاف السلوك الشاذ وتدهور الخدمة في الوقت المناسب. يلعب برنامج المراقبة وتسجيل الدخول دورًا رئيسيًا في هذا الجانب من الأمان، حيث يوفر نظرة ثاقبة لما يحدث على النظام والشبكة.

في هذا القسم، سنراجع بعض الأدوات التي يمكن استخدامها لمراقبة العديد من جوانب نظام كالي.

١.٥.٧. مراقبة السجلات باستخدام logcheck

يراقب برنامج **`logcheck`** ملفات السجل كل ساعة بشكل افتراضي ويرسل رسائل سجل غير عادية في رسائل البريد الإلكتروني إلى المسؤول لمزيد من التحليل.

يتم تخزين قائمة الملفات المراقبة في /etc/logcheck/logcheck.logfiles. تعمل القيم الافتراضية بشكل جيد إذا لم يتم إصلاح الملف /etc/rsyslog.conf بالكامل.

logcheck يمكن أن يقدم تقرير تسجيل الدخول مستويات مختلفة من التفاصيل:

شكوك الخادم ومحطة العمل. وشكوك مطوّلة جدًا، وربما يجب أن يقتصر على خوادم محددة مثل: جدران الحماية. *الخادم* هو الوضع الافتراضي ويوصى به لمعظم الخوادم. من الواضح أن *محطة العمل* مصممة لمحطات العمل وهي مقتضبة للغاية، حيث تقوم بتصفية رسائل أكثر من الخيارات الأخرى.

في جميع الحالات الثلاث، ربما يجب تخصيص **logcheck** لاستبعاد بعض الرسائل الإضافية (اعتمادًا على الخدمات المثبتة)، ما لم ترغب حقًا في تلقي دفعات كل ساعة من رسائل البريد الإلكتروني الطويلة غير المثيرة للاهتمام. نظرًا لأن آلية اختيار الرسائل معقدة نوعًا ما، فإن قراءة /usr/share/doc/logcheck-database/README.logcheck-database.gz/ مطلوبة - إذا كانت صعبة - للقراءة.

يمكن تقسيم القواعد المطبقة إلى عدة أنواع:

- تلك التي تعتبر رسالة كمحاولة اختراق (مخزنة في ملف في /etc/logcheck/cracking.d/directory/).
- محاولات الاختراق المتجاهلة (/etc/logcheck/cracking.ignore.d/).
- الرسائل المصنفة على أنها تنبيه أمان (/etc/logcheck/violations.d/).
- تنبيهات الأمان التي تم تجاهلها (/etc/logcheck/violations.ignore.d/).
- أخيرًا، الرسائل المتبقية (تعتبر أحداث النظام).

يتم استخدام ملفات ignore.d لتجاهل (من الواضح) الرسائل. على سبيل المثال، لا يمكن تجاهل رسالة تم وضع علامة عليها كمحاولة اختراق أو تنبيه أمان (باتباع قاعدة مخزنة في ملف **etc/logcheck/violations.d/myfile**) إلا من خلال قاعدة في ملف **/etc/logcheck/violations.ignore.d/myfile** أو ملف **/etc/logcheck/violations.ignore.d/myfile**-*extension*.

يتم دائمًا الإشارة إلى حدث النظام ما لم تنص القاعدة في أحد مجلدات **/etc/logcheck/ignore.d.{paranoid,server,workstation}/** على أنه يجب تجاهل الحدث. بالطبع، المجلدات الوحيدة التي تم أخذها في الاعتبار هي تلك التي تتوافق مع مستويات الإسهاب مساوية أو أكبر من وضع التشغيل المحدد.

٢.٥.٧. مراقبة النشاط في الوقت الحقيقي

top هي أداة تفاعلية تعرض قائمة بالعمليات الجارية حاليًا. يعتمد الفرز الافتراضي على المقدار الحالي لاستخدام المعالج ويمكن الحصول عليه باستخدام المفتاح P. تتضمن أوامر الفرز الأخرى الفرز حسب الذاكرة المشغولة (المفتاح M)، حسب إجمالي وقت المعالج (المفتاح T)، ومعرف العملية (المفتاح N). يقتل المفتاح k العملية بإدخال معرف العملية الخاص بها. يغير المفتاح r أولوية العملية.

عندما يبدو النظام مثقلاً، فإن **top** هي أداة رائعة لمعرفة العمليات التي تتنافس على وقت المعالج أو تستهلك الكثير من الذاكرة. على وجه الخصوص، من المثير للاهتمام غالبًا التحقق مما إذا كانت العمليات التي تستهلك الموارد تتطابق مع الخدمات الحقيقية التي من المعروف أن الجهاز يستضيفها. هناك عملية غير معروفة تعمل كمستخدم "www-data" يجب أن تبرز حقًا ويتم التحقيق فيها نظرًا لأنها على الأرجح نسخة من برنامج تم تثبيته وتنفيذه على النظام من خلال ثغرة أمنية في تطبيق ويب.

top أداة مرنة للغاية وتعطي الصفحة اليدوية تفاصيل حول كيفية تخصيص شاشتها وتكييفها مع احتياجاتك وعاداتك الشخصية.

gnome-system-monitor مشابهة لـ **top** وتوفر نفس الميزات تقريبًا.

٣.٥.٧. كشف التغييرات

بمجرد تثبيت النظام وتكوينه، يجب أن تظل معظم ملفات النظام ثابتة نسبيًا حتى تتم ترقية النظام. لذلك، من الجيد مراقبة التغييرات في ملفات النظام حيث أن أي تغيير غير متوقع قد يكون سببًا للقلق ويجب التحقيق فيه. يقدم هذا القسم بعضًا من الأدوات الأكثر شيوعًا المستخدمة لمراقبة ملفات النظام واكتشاف التغييرات وإعلامك اختياريًا كمسؤول عن النظام.

١.٣.٥.٧. تدقيق حزم بـ dpkg --verify

dpkg --verify (أو **dpkg -V**) هي أداة مثيرة للاهتمام لأنها تعرض ملفات النظام التي تم تعديلها (ربما من قبل مهاجم)، ولكن هذا الإخراج يجب أن يؤخذ على محمل الشك. للقيام بعملها، يعتمد dpkg على المجموع الاختباري المخزن في قاعدة البيانات الخاصة به والتي يتم تخزينها على القرص الصلب (الموجود في **/var/lib/dpkg/info/package.md5sums**). سيعدل المهاجم هذه الملفات بحيث تحتوي على المجموع الاختباري الجديد للملفات المخربة، أو سيهاجم المهاجم متقدم الحزمة الموجودة على مرآة دبيان الخاصة بك. للحماية من هذه الفئة من الهجمات، استخدم نظام التحقق من التوقيع الرقمي لـ APT (انظر القسم ٦.٣.٨، "التحقق من صحة الحزمة") للتحقق من صحة الحزم بشكل صحيح.

ما هي بصمة الملف؟

للتذكير: بصمة الإصبع هي قيمة، غالبًا رقم (على الرغم من ذلك في تدوين سداسي عشري)، يحتوي على نوع من التوقيع لمحتويات الملف. يتم حساب هذا التوقيع باستخدام خوارزمية (تكون MD5 أو SHA1 أمثلة معروفة جيدًا) تضمن بشكل أو بآخر أنه حتى أصغر تغيير في محتويات الملف سيؤدي إلى تغيير بصمة الإصبع؛ يُعرف هذا باسم "تأثير الانهيار الجليدي". ثم تعمل البصمة العددية البسيطة كاختبار عباد الشمس للتحقق مما إذا تم تغيير محتويات الملف. هذه الخوارزميات غير قابلة للعكس. بعبارة أخرى، بالنسبة لمعظمهم، فإن معرفة بصمة الإصبع لا تسمح بالعثور على المحتويات المقابلة. يبدو أن التطورات الرياضية الأخيرة تضعف من استبداد هذه المبادئ ولكن استخدامها ليس موضع تساؤل حتى الآن، حيث أن إنشاء محتويات مختلفة تعطي نفس بصمة الإصبع لا يزال يبدو مهمة صعبة للغاية.

سيؤدي تشغيل dpkg -V إلى التحقق من جميع الحزم المثبتة وسيطبع سطراً لكل ملف يفشل في التحقق. يشير كل حرف إلى اختبار على بعض بيانات التعريف المحددة. لسوء الحظ، لا يقوم dpkg بتخزين البيانات الوصفية اللازمة لمعظم الاختبارات وبالتالي سيخرج علامات استفهام لهم. حاليا فقط اختبار المجموع الاختباري يمكن أن يعطي 5 على الحرف الثالث (عندما يفشل).

```
# dpkg -V
??5??????   /lib/systemd/system/ssh.service
??5?????? c /etc/libvirt/qemu/networks/default.xml
??5?????? c /etc/lvm/lvm.conf
??5?????? c /etc/salt/roster
```

في المثال أعلاه، يبلغ **dpkg** عن تغيير في ملف خدمة SSH قام به المسؤول للملف الذي تم حزمه بدلاً من استخدام تجاوز etc/systemd/system/ssh.service/ مناسب (والذي سيتم تخزينه أدناه **etc/** مثل أي تغيير في التكوين يجب يكون). يسرد أيضًا العديد من ملفات التهيئة (المحددة بحرف "c" في الحقل الثاني) التي تم تعديلها بشكل قانوني.

٢.٣.٥.٧. ملفات المراقبة: AIDE

تقوم أداة بيئة اكتشاف التطفل المتقدمة "Advanced Intrusion Detection Environment" (AIDE) بفحص تكامل الملف واكتشاف أي تغيير مقابل صورة مسجلة مسبقًا للنظام الصالح. يتم تخزين الصورة كقاعدة بيانات (var/lib/aide/aide.db/) تحتوي على المعلومات ذات الصلة في جميع ملفات النظام (بصمات الأصابع والأذونات والطوابع الزمنية وما إلى ذلك).

يمكنك تثبيت AIDE عن طريق تشغيل **apt update** متبوعًا بـ **apt install aide**. ستقوم أولاً بتهيئة قاعدة البيانات باستخدام **aideinit**؛ سيتم تشغيله يوميًا (عبر البرنامج النصي /etc/cron.daily/aide) للتحقق من عدم تغير أي شيء ذي صلة. عندما يتم الكشف عن التغييرات، يقوم AIDE بتسجيلها في ملفات السجل (/var/log/aide/*.log) ويرسل نتائجها إلى المسؤول عن طريق البريد الإلكتروني.

حماية قاعدة البيانات

نظرًا لأن AIDE تستخدم قاعدة بيانات محلية لمقارنة حالات الملفات، فإن صحة نتائجها ترتبط مباشرةً بصحة قاعدة البيانات. إذا حصل المهاجم على أذونات الجذر لنظام مخترق، فسيكون قادرًا على استبدال قاعدة البيانات وتغطية مساراته. تتمثل إحدى طرق منع هذا التخريب في تخزين البيانات المرجعية على وسائط تخزين للقراءة فقط.

يمكنك استخدام الخيارات في **/etc/default/aide** لتعديل سلوك الحزمة المساعدة. يتم تخزين تكوين AIDE المناسب في **/etc/aide/aide.conf** و **/etc/aide/aide.conf.d/** (في الواقع، يتم استخدام هذه الملفات فقط من خلال **update-aide.conf** لإنشاء **/var/lib/aide/aide.conf.autogenerated**). يشير التكوين إلى خصائص الملفات التي يجب التحقق منها. على سبيل المثال، تتغير محتويات ملفات السجل بشكل روتيني، ويمكن تجاهل هذه التغييرات طالما بقيت أذونات هذه الملفات كما هي، ولكن يجب أن تكون محتويات وأذونات البرامج القابلة للتنفيذ ثابتة. على الرغم من أنها ليست معقدة للغاية، إلا أن بنية التكوين ليست بديهية بالكامل ونوصي بقراءة صفحة الدليل (5) aide.conf لمزيد من التفاصيل.

يتم إنشاء نسخة جديدة من قاعدة البيانات يومياً في var/lib/aide/aide.db.new/ ؛ إذا كانت جميع التغييرات المسجلة شرعية، يمكن استخدامها لاستبدال قاعدة البيانات المرجعية.

Tripwire يشبه إلى حد بعيد AIDE، حتى بنية ملف التكوين هي نفسها تقريبًا. الإضافة الرئيسية التي توفرها tripwire هي آلية لتوقيع ملف التكوين بحيث لا يتمكن المهاجم من جعله يشير إلى نسخة مختلفة من قاعدة البيانات المرجعية.

يقدم **Samhain** أيضًا ميزات مشابهة بالإضافة إلى بعض الوظائف للمساعدة في الكشف عن الجذور الخفية. يمكن أيضًا نشره عالميًا على شبكة وتسجيل آثاره على خادم مركزي (بتوقيع).

checksecurity وحزم chkrootkit/rkhunter

يتكون **checksecurity** من العديد من البرامج النصية الصغيرة التي تقوم بإجراء الفحوصات الأساسية على النظام (البحث عن كلمات المرور الفارغة والملفات setuid الجديدة وما إلى ذلك) وتحذيرك إذا تم الكشف عن هذه الشروط. على الرغم من اسمه الصريح، لا يجب الاعتماد عليه فقط للتأكد من أن نظام Linux آمن.
تكتشف حزم chkrootkit و rkhunter بعض الجذور الخفية التي يمكن تثبيتها على النظام. للتذكير، هذه هي قطع من البرامج المصممة لإخفاء اختراق النظام مع الحفاظ على التحكم في الجهاز بسرية. الاختبارات ليست موثوقة بنسبة ١٠٠ في المائة ولكنها عادة ما تلفت انتباهك إلى المشاكل المحتملة.

٦.٧. ملخص

في هذا الفصل، ألقينا نظرة على مفهوم السياسات الأمنية، وأبرزنا النقاط المختلفة التي يجب مراعاتها عند تحديد مثل هذه السياسة وتحديد بعض التهديدات لنظامك ولشخصك كمحترف أمني. ناقشنا التدابير الأمنية للحاسوب المحمول وسطح المكتب بالإضافة إلى الجدران النارية وتصفية الحزم. أخيرًا، راجعنا أدوات واستراتيجيات المراقبة وأظهرنا كيفية تنفيذها بشكل أفضل للكشف عن التهديدات المحتملة لنظامك.

نصائح تلخيصية:

خصص بعض الوقت لتحديد سياسة أمنية شاملة.

إذا كنت تقوم بتشغيل Kali على خادم يمكن الوصول إليه بشكل عام، فقم بتغيير أي كلمات مرور افتراضية للخدمات التي يمكن تكوينها (انظر القسم ٣.٧، "تأمين خدمات الشبكة") وقم بتقييد وصولهم بجدار حماية (انظر القسم ٤.٧، "جدار الحماية أو تصفية الحزم") قبل إطلاقها.

استخدم **`fail2ban`** لاكتشاف وحظر هجمات تخمين كلمة المرور وهجمات كلمة مرور القوة الغاشمة عن بُعد.

إذا قمت بتشغيل خدمات الويب، استضفها عبر HTTPS لمنع وسطاء الشبكة من استنشاق حركة المرور الخاصة بك (والتي قد تتضمن ملفات تعريف ارتباط المصادقة).

غالبًا ما تنشأ المخاطر الحقيقية عند السفر من عميل إلى آخر. على سبيل المثال، يمكن سرقة الحاسوب المحمول أثناء السفر أو الاستيلاء عليه من قبل الجمارك. استعد لهذه الاحتمالات المؤسفة باستخدام التشفير الكامل للقرص (انظر القسم ٢.٢.٤، "التثبيت على نظام ملفات مشفر بالكامل") وفكر في ميزة **nuke** (انظر إضافة كلمة مرور Nuke لمزيد من الأمان) لحماية بيانات عملائك.

قم بتطبيق قواعد جدار الحماية (انظر القسم ٤.٧، "جدار الحماية أو تصفية الحزم") لمنع كل حركة المرور الصادرة باستثناء حركة المرور الناتجة عن وصول VPN الخاص بك. يُقصد بهذا شبكة أمان، بحيث عندما تعطل الشبكة الافتراضية الخاصة، ستلاحظها على الفور (بدلاً من العودة إلى الوصول إلى الشبكة المحلية).

قم بتعطيل الخدمات التي لا تستخدمها. يُسهل كالي القيام بذلك نظرًا لأن جميع خدمات الشبكة الخارجية معطلة افتراضيًا.

يشتمل نواة Linux على جدار الحماية **netfilter**. لا يوجد حل جاهز لتكوين أي جدار حماية، حيث تختلف متطلبات الشبكة والمستخدم. ومع ذلك، يمكنك التحكم في **netfilter** من مساحة المستخدم باستخدام أوامر **iptables** و **ip6tables**.

يراقب برنامج **logcheck** ملفات السجل كل ساعة بشكل افتراضي ويرسل رسائل سجل غير عادية في رسائل البريد الإلكتروني إلى المسؤول لمزيد من التحليل.

top هي أداة تفاعلية تعرض قائمة بالعمليات الجارية حاليًا.

يعرض **dpkg --verify** (أو **dpkg -V**) ملفات النظام التي تم تعديلها (من المحتمل من قبل مهاجم)، ولكنها تعتمد على المجموع الاختباري، والذي قد يتم تخريبه من قبل مهاجم ذكي.

تحقق أداة بيئة كشف التسلل المتقدمة (**AIDE**) من سلامة الملف وتكتشف أي تغييرات مقابل صورة مسجلة مسبقًا للنظام الصالح.

يشبه Tripwire إلى حد كبير AIDE ولكنه يستخدم آلية لتوقيع ملف التكوين، بحيث لا يتمكن المهاجم من جعله يشير إلى إصدار مختلف من قاعدة البيانات المرجعية.

ضع في اعتبارك استخدام **rkhunter** و **checkecurity** و **chkrootkit** للمساعدة في الكشف عن الجذور الخفية على نظامك.

في الفصل التالي، سنبحث في أساسيات دبيان وإدارة الحزم. ستفهم بسرعة القوة الكامنة وراء جذور ديبيان في كالي وستتعلم كيف استغل المطورون تلك القوة. كن حذرًا، الفصل التالي كثيف إلى حد ما، ولكن من المهم أن تفهم أساسيات دبيان وإدارة الحزم إذا كنت ستصبح مستخدمًا قويًا في كالي.

التمرين الأول للفصل السابع - تأمين شبكة كالي

١. حدد جميع المنافذ المفتوحة على نظام كالي الخاص بك.

٢. قم بتكوين جدار الحماية Kali الخاص بك للسماح باتصالات TCP الواردة على المنافذ 22 و 80 و 443 فقط.

٣. تحقق من حظر المنافذ الأخرى باستخدام أداة مساعدة مثل netcat.

٤. تأكد من استمرار هذه القواعد بعد إعادة التشغيل. إعادة التشغيل للتحقق!

الإجابات:

١. تحقق من المنافذ المفتوحة

```
root@kali:~# netstat -tulpen
root@kali:~# iptables -n -L INPUT
```

إذا كان لديك منافذ قمت بحظرها، أو قواعد iptables السابقة، يمكنك إسقاطها جميعًا:

```
root@kali:~# iptables -F INPUT
root@kali:~# iptables -P INPUT ACCEPT
root@kali:~# iptables -P FORWARD ACCEPT
root@kali:~# iptables -P OUTPUT ACCEPT
```

تحقق الآن لمعرفة ما إذا كان يمكنك الاتصال بالمنفذ 4444 على جهازك عن طريق تشغيل **netcat** بالطريقة التالية. لاحظ أنه في هذا التمرين، ستختلف عناوين IP الخاصة بك بالطبع:

```
root@kali:~# nc -lnvp 4444
listening on [any] 4444 ...
```

من الجهاز المضيف أو جهاز آخر، حاول الاتصال بمثيل **netcat** للاستماع. بمجرد الاتصال، اكتب بعض الأحرف، ويجب أن تظهر في مستمع Kali VM nc:

```
root@HOST_MACHINE:~#  nc -v 172.16.161.136 4444
aaaaaaaa
```

ملاحظة: إذا كنت لا ترى الأحرف التي كتبتها في مستمع Kali nc، فهناك مشكلة. احصل على حل قبل المتابعة. إذا كنت في VM، فقم بالتبديل إلى الشبكات الموصولة " bridged networking" بدلاً من NAT، إلخ حتى يعمل هذا المثال nc.

٢. قم بتكوين جدار الحماية باستخدام أوامر مشابهة لما يلي:

```
iptables -P INPUT DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
```

تحقق الآن لمعرفة ما إذا كان يمكنك الاتصال بالمنفذ 4444 على الجهاز ذي الجدار الناري عن طريق تشغيل **netcat** بالطريقة التالية:

```
root@kali:~# nc -lvp 4444
listening on [any] 4444 ...
```

٣. من الجهاز المضيف، حاول الاتصال بمثيل **netcat** للاستماع. يجب أن تفشل:

```
root@HOST_MACHINE:~# nc -v 172.16.161.136 4444
nc: connectx to 172.16.161.136 port 4444 (tcp) failed: Operation timed out
```

٤. الآن ، قم بإنشاء برنامج نصي iptables من هذه القواعد:

```
root@kali:~# iptables-save  > /usr/local/etc/myconfig.fw
```

وتسجيل البرنامج النصي للتكوين في التوجيه المسبق لملف /etc/network/interfaces. إعادة التشغيل لمعرفة ما إذا كانت القواعد لا تزال قائمة!

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
pre-up iptables-restore < /usr/local/etc/myconfig.fw
```

التمرين الثاني للفصل السابع – مراقبة خوادم كالي

١. قم بتثبيت **logcheck** على مثيل Kali الخاص بك

٢. جرّب استخدام خدمة SSH الخاصة بك، واكتشف ما إذا كان فحص السجل يلتقط ذلك، ويبلغ عن الهجوم.

٣. قم بإنشاء نسخة cron’ed من **logcheck**، بحيث يتم تشغيله مرة واحدة في الساعة، وإنشاء ملف سجل في data/$(date-time).log/

الإجابات:

١. قم بتثبيت **logcheck** وشغله للمرة الأولى:

```
apt-get install logcheck
sudo -u logcheck logcheck –o
```

٢. قم بتنزيل قائمة كلمات المرور، وقم بإجبار خدمة SSH الخاصة بك باستخدام hydra، وتحقق من أن تسجيل الدخول يقوم بالإبلاغ عنها:

```
wget
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/500-worst-passwords.txt
hydra -l root -P 500-worst-passwords.txt 127.0.0.1 ssh
tail -f /var/log/auth.log
sudo -u logcheck logcheck –o
```

٣. بعد ذلك، اكتب نص برمجي Bash مشابه لما يلي:

```
mkdir -p /data/
sudo -u logcheck logcheck -o > /data/$(date +"%m-%d-%Y-%T").log
```

اجعله قابل للتنفيذ وأفلته في /etc/cron.hourly.

التمرين الثالث للفصل السابع - تأمين نظام الملفات

قم بتثبيت **`tripwire`** على جهاز Kali الخاص بك. راقب المجلد /var/www/html للتعرف على التغييرات.

إذا فعلت كل شيء بشكل صحيح، فستحصل على الكثير من "أخطاء نظام الملفات". هل أنت hax0red؟ في كلتا الحالتين، قم بإصلاحه.

الإجابات:

١. قم بتثبيت tripwire وتكوين الملفات التي تريد حمايتها:

apt-get install tripwire # yes, yes, yes, yes

nano /etc/tripwire/twpol.txt # list the directories and files you want to protect

أضف كتلة التعليمات البرمجية التالية في ملف سياسة **tripwire**:

```
# Webserver file and folder monitoring
(
  rulename = "Web server file and directories",
  severity = $(SIG_HI)
)
{
        /var/www/html    -> $(SEC_BIN);
}
```

تحقق الآن من أن tripwire يتم التقاط أي تغييرات في var/www/html:

```
twadmin -m P /etc/tripwire/twpol.txt #Create Policy File
tripwire --init #Initialize database
tripwire --check #Initial integrity check
touch /var/www/html/shell_backdoor.php
tripwire --check
tripwire --update-policy -Z low /etc/tripwire/twpol.txt
tripwire --check
```

٢. السر موجود في ملف سياسة etc/tripwire/twpol.txt/. امسح السطور التي تقوم بإظهار الأخطاء. اعتبارًا من وقت كتابة هذا التقرير، قد تتضمن الملفات:

- /etc/rc.boot
- /root/mail
- /root/Mail
- /root/.xsession-errors
- /root/.xauth
- /root/.tcshrc
- /root/.sawfish
- /root/.pinerc

- /root/.mc
- /root/.gnome_private
- /root/.gnome-desktop
- /root/.gnome
- /root/.esd_auth
- /root/.elm
- /root/.cshrc
- /root/.bash_profile
- /root/.bash_logout
- /root/.amandahosts
- /root/.addressbook.lu
- /root/.addressbook
- /root/.Xresources
- /root/.Xauthority

بمجرد تغيير هذا الملف، يجب عليك تحديث ملف السياسة وتشغيل الفحص مرة أخرى:

```
tripwire --update-policy -Z low /etc/tripwire/twpol.txt
#Update Policy File
tripwire --check
```

غذاء الفكر

إليك استخدام رائع ومثير للاهتمام من **iptables**. يمكنك تحويل أي حاسوب بواجهة لاسلكية إلى نقطة وصول لاسلكية بـ **hostapd**. يأتي هذا الحل من هنا:

```
iptables -t nat -F
iptables -F
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
echo '1' > /proc/sys/net/ipv4/ip_forward
(DNS, dhcp still required)
```

أيضا، تحقق من هذا الدليل المرجعي الرائع لـ **iptables**.

https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands

اختبار الشهادة للفصل السابع

١. حدد جميع وظائف الأمان المدمجة للتثبيت الافتراضي لـ Kali Linux:

- o لم يتم تمكين أي خدمات بشكل افتراضي
- o تجزئة امتيازات الخدمة
- o تم تمكين جدار الحماية الذي تم تكوينه مسبقًا
- o تميل جميع الخدمات إلى بيانات الاعتماد غير الافتراضية

٢. أي مما يلي مرتبط بجدار حماية Kali Linux؟ اختر كل ما ينطبق.

- o netfilter
- o fwbuilder
- o ip6tables
- o iptables

٣. أي مما يلي هو سلسلة افتراضية في جدار الحماية Kali Linux؟

- o ALL
- o DROP
- o FILTER
- o INPUT
- o RAW

٤. أي من الإجراءات التالية لجدار حماية Kali Linux لن يتداخل مع الحزم التي يتم التعامل معها؟

- OUTPUT
- LOG
- ULOG
- SNAT
- ACCEPT

٥. رتب السلاسل في ترتيب المعالجة الصحيح، من الأول إلى الأخير:

- ☐ PREROUTING
- ☐ POSTROUTING
- ☐ INPUT
- ☐ FORWARD
- ☐ OUTPUT

٦. أي مما يلي سيطبق حالة خاصة من مصدر NAT على الحزم في جدار حماية Kali Linux؟

- SOURCE
- MASQUERADE
- DNAT
- POSTROUTE

٧. أي من الأوامر التالية سيمنع جميع الحزم التي تبدأ من ٨.٨.٨.٨؟

- o iptables -A OUTPUT -s 8.8.8.8 -j DROP
- o iptables -A INPUT -s 8.8.8.8 -j DROP
- o iptables -A INPUT -s 8.8.8.8 -t ALL -j DROP
- o iptables -A ALL -s 8.8.8.8 -j DROP

٨. أي من الأوامر التالية يستخدم لحذف جميع القواعد في سلسلة INPUT؟

- o iptables -X INPUT
- o iptables -F INPUT
- o iptables -D INPUT
- o iptables -R INPUT

٩. أي مما يلي سيسمح صراحة باتصالات SSH بجهاز Kali Linux؟

- o iptables -A INPUT -p ssh -j ACCEPT
- o iptables -A INPUT –dport 22 -j ACCEPT
- o iptables -A INPUT –state NEW -p tcp –dport 22 -j ACCEPT
- o iptables -A INPUT -m state –state NEW -p tcp –dport 22 -j ACCEPT

١٠. ما الملف الذي يجب تحديثه لتمكين قواعد جدار الحماية المخصصة في وقت الإقلاع؟

- /etc/netfilter.conf
- /etc/network/interfaces
- /etc/init.d/netfilter
- /etc/netfilter/netfilter.conf

١١. ما الأداة التي يمكن استخدامها لمراقبة حالة العملية رسوميا؟

- ps -ax
- System Monitor
- ntop
- gnome-system-monitor

١٢. أي أمر سهل التخريب يمكن استخدامه للكشف عن الحزم المشبوهة؟

- dpkg –V
- dpkg -l
- dpkg -v
- dpkg –checksum

١٣. أي مما يلي يمكن استخدامه للحماية من عمليات تسجيل الدخول القوة الغاشمة؟

- logcheck
- AIDE
- tripwire
- fail2ban

الإجابات:

١. لم يتم تمكين أي خدمات بشكل افتراضي

٢. كل الخيارات

3. INPUT
4. LOG, ULOG, ACCEPT.
5. PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING
6. MASQUERADE
7. iptables -A INPUT -s 8.8.8.8 -j DROP
8. iptables -F INPUT
9. iptables -A INPUT -m state –state NEW -p tcp –dport 22 -j ACCEPT
10. /etc/network/interfaces
11. gnome-system-monitor
12. dpkg -V
13. fail2ban

---((الفصل الثامن))---

٨. إدارة حزم Debian

بعد أساسيات لينكس، حان الوقت لتعلم نظام إدارة حزم التوزيعات المستندة على دبيان. في مثل هذه التوزيعات، بما في ذلك كالي، تعتبر حزمة دبيان الطريقة الأساسية لإتاحة البرامج للمستخدمين النهائيين. سيمنحك فهم نظام إدارة الحزم قدرًا كبيرًا لمعرفة كيفية بناء Kali، وتمكنك من استكشاف المشكلات بشكل أكثر فعالية، ومساعدتك في تحديد موقع المساعدة والوثائق بسرعة لمجموعة كبيرة من الأدوات والأدوات المساعدة المضمنة في Kali Linux.

في هذا الفصل، سوف نقدم نظام إدارة حزم دبيان ونقدم مجموعة أدوات **dpkg** ومجموعة APT. تكمن إحدى نقاط القوة الأساسية لـ Kali Linux في مرونة نظام إدارة الحزم الخاص به، والذي يستفيد من هذه الأدوات لتوفير التثبيت شبه الكامل، والترقية، والإزالة، والتلاعب ببرامج التطبيق، وحتى نظام التشغيل الأساسي نفسه. من المهم أن تفهم كيف يعمل هذا النظام لتحقيق أقصى استفادة من كالي وتبسيط جهودك. لقد ولت أيام التجميعات المؤلمة، والترقيات الكارثية، وتصحيح الأخطاء **gcc**، **make**، و"**configure**" تكوين المشكلات، ومع ذلك، فقد انفجر عدد التطبيقات المتاحة وتحتاج إلى فهم الأدوات المصممة للاستفادة منها. هذه أيضًا مهارة مطلوبة؛ نظرًا لوجود عدد من أدوات الأمان التي لا يمكن تضمينها في Kali بسبب الترخيص أو مشكلات أخرى ولكن توفر حزم دبيان للتنزيل. من المهم أن تعرف كيفية معالجة هذه الحزم وتثبيتها وكيف تؤثر على النظام، خاصة عندما لا تسير الأمور كما هو متوقع.

سنبدأ ببعض النظرات العامة الأساسية لـ APT، ونصف هيكل ومحتويات الحزم الثنائية والمصدر، ونلقي نظرة على بعض الأدوات والسيناريوهات الأساسية، ثم نتعمق أكثر لمساعدتك في فهم كل قطعة من الأداة المساعدة من نظام الحزمة والتركيبة المذهلين من الأدوات.

١.٨. مقدمة في APT

لنبدأ ببعض التعريفات الأساسية، ونظرة عامة، وبعض التاريخ عن حزم دبيان، بدءًا من **dpkg** و APT.

١.١.٨. العلاقة بين APT و dpkg

حزمة دبيان عبارة عن أرشيف مضغوط لتطبيق برمجي. تحتوي *الحزمة الثنائية "binary package"* (ملف **deb.**) على ملفات يمكن استخدامها مباشرة (مثل البرامج أو الوثائق)، بينما تحتوي *الحزمة المصدر "source package"* على الكود المصدري للبرنامج والتعليمات المطلوبة لبناء حزمة ثنائية. تحتوي حزمة دبيان على ملفات التطبيق بالإضافة إلى البيانات الوصفية الأخرى بما في ذلك أسماء التبعيات التي يحتاجها التطبيق، بالإضافة إلى النصوص البرمجية التي تمكن من تنفيذ الأوامر في مراحل مختلفة من دورة حياة الحزمة (التثبيت والإزالة والترقيات).

تم تصميم أداة **dpkg** لمعالجة حزم **deb.** وتثبيتها، ولكن إذا واجهت تبعية غير مرضية (مثل مكتبة مفقودة) تمنع التثبيت من الحزمة، فسوف يسرد **dpkg** ببساطة التبعية المفقودة، لأنه ليس لديه وعي أو مدمج في المنطق للعثور على الحزم التي قد تلبي تلك التبعيات أو معالجتها. تم تصميم أداة الحزمة المتقدمة (APT)، بما في ذلك **apt** و **apt-get**، لمعالجة هذه العيوب ويمكنها حل هذه المشكلات تلقائيًا. سنتحدث عن كل من أدوات **dpkg** وأدوات APT في هذا الفصل.

الأمر الأساسي للتعامل مع حزم دبيان على النظام هو **dpkg**، الذي يقوم بتثبيت أو تحليل حزم **.deb** ومحتوياتها. ومع ذلك، فإن **dpkg** لديه رؤية جزئية فقط لعالم دبيان: فهو يعرف ما هو مثبت على النظام وما تقدمه في سطر الأوامر، ولكنه لا يعرف شيئًا عن الحزم الأخرى المتاحة. على هذا النحو، ستفشل إذا لم يتم تلبية التبعية. تعالج APT القيود.

APT هي مجموعة من الأدوات التي تساعد على إدارة حزم دبيان أو التطبيقات على نظام دبيان الخاص بك. يمكنك استخدام APT لتثبيت التطبيقات وإزالتها وتحديث الحزم وحتى ترقية نظامك بالكامل. يكمن سحر APT في الحقيقة أنه نظام إدارة حزم كامل لن يقوم فقط بتثبيت حزمة أو إزالتها، بل سيأخذ بعين الاعتبار متطلبات واعتمادات التطبيق المعبأ (وحتى متطلباتها وتبعياتها) ويحاول تلبيتها تلقائيا. تعتمد APT على **dpkg** لكن APT تختلف عن **dpkg**، حيث تقوم الأولى بتثبيت أحدث حزمة من المصدر عبر الإنترنت وتعمل على حل التبعيات بينما يقوم **dpkg** بتثبيت حزمة موجودة على نظامك المحلي ولا يحل التبعيات تلقائيًا.

إذا كنت قد قضيت وقتًا كافيًا لتذكر تجميع البرامج باستخدام **gcc** (حتى بمساعدة أدوات مساعدة مثل **make** و**configure**)، فمن المحتمل أن تتذكر أنها كانت عملية مؤلمة، خاصة إذا كان التطبيق يحتوي على عدة تبعيات. من خلال فك تشفير التحذيرات ورسائل الخطأ المختلفة، قد تتمكن من تحديد أي جزء من التعليمات البرمجية كان يفشل وغالباً ما يكون هذا الفشل بسبب مكتبة مفقودة أو تبعية أخرى. يمكنك بعد ذلك تعقب تلك المكتبة المفقودة أو التبعية وتصحيحها والمحاولة مرة أخرى. بعد ذلك، إذا كنت محظوظًا، فستكتمل المجموعة، ولكن غالبًا ما يفشل البناء مرة أخرى، ويشكو من تبعية أخرى مكسورة.

تم تصميم APT للمساعدة في التخفيف من هذه المشكلة، وجمع متطلبات البرنامج وتبعياته، وحلها. تعمل هذه الوظيفة من خارج الصندوق على Kali Linux، ولكنها ليست مضمونة. من المهم أن تفهم كيف يعمل نظام التعبئة الخاص بـ Debian وKali؛ لأنك ستحتاج إلى تثبيت الحزم أو تحديث البرامج أو استكشاف مشكلات الحزم وإصلاحها. ستستخدم APT في عملك اليومي مع Kali Linux وفي هذا الفصل، سوف نقدم لك APT وسنوضح لك كيفية تثبيت الحزم وإزالتها وترقيتها وإدارتها، بل نوضح لك أيضًا كيفية نقل الحزم بين توزيعات لينكس مختلفة. سنتحدث أيضًا عن الأدوات الرسومية التي تعزز APT، ونوضح لك كيفية التحقق من صحة الحزم، والتعمق في مفهوم التوزيع المستمر "rolling distribution"، وهي تقنية تجلب تحديثات يومية إلى نظام Kali الخاص بك.

قبل أن نتقدم ونوضح لك كيفية استخدام **dpkg** و APT لتثبيت الحزم وإدارتها، من المهم أن نتعمق في بعض الأعمال الداخلية لـ APT ونناقش بعض المصطلحات المحيطة بها.

> **مصدر الحزمة وحزمة المصدر**
>
> يمكن أن يكون مصدر الكلمة غامضًا. يجب عدم الخلط بين حزمة المصدر -حزمة تحتوي على الكود المصدري لبرنامج- مع مصدر الحزمة -مستودع (موقع ويب، خادم FTP، قرص مضغوط، مجلد محلي ، إلخ) يحتوي على حزم.

تسترد APT حزمها من مستودع أو نظام تخزين حزم أو ببساطة من "مصدر الحزمة". يسرد ملف **/etc/apt/sources.list** المستودعات (أو المصادر) المختلفة التي تنشر حزم دبيان.

٢.١.٨. فهم ملف sources.list

ملف **sources.list** هو ملف التكوين الأساسي لتحديد مصادر الحزمة، ومن المهم فهم كيفية وضعه وكيفية تكوينه؛ لأن APT لن تعمل بدون قائمة محددة بشكل صحيح لمصادر الحزمة. دعنا نناقش تركيبتها، ونلقي نظرة على المستودعات المختلفة التي يستخدمها Kali Linux، ونناقش المرايا وإعادة التوجيه، ثم ستكون جاهزاً لاستخدام APT.

يحتوي كل سطر نشط من ملف **/etc/apt/sources.list** (وملفات **/etc/apt/sources.list.d/*.list**) على وصف مصدر، مكون من ثلاثة أجزاء مفصولة بمسافات. تبدأ الأسطر المُعلّقة بعلامة #:

deb cdrom:[Debian GNU/Linux 2016.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20160830-11:29]/ kali-rolling contrib main non-free

deb http://http.kali.org/kali kali-rolling main non-free contrib

دعنا نلقي نظرة على تركيب هذا الملف. يشير الحقل الأول إلى نوع المصدر:

deb للحزم الثنائية،

deb-src لحزم المصدر.

يعطي الحقل الثاني عنوان URL الأساسي للمصدر: يمكن أن يتكون هذا من مرآة دبيان أو أي أرشيف حزم آخر تم إعداده من قبل طرف ثالث. يمكن أن يبدأ عنوان URL بـ **//:file** للإشارة إلى مصدر محلي مثبت في التسلسل الهرمي لملفات النظام، أو **//:http** للإشارة إلى مصدر يمكن الوصول إليه من خادم ويب، أو باستخدام **//:ftp** لمصدر متوفر على خادم FTP. يمكن أن يبدأ عنوان URL أيضًا بـ **:cdrom** لعمليات التثبيت التي تستند إلى قرص CD-ROM/DVD-ROM/Blu-ray، على الرغم من أن هذا أقل إستخداما؛ لأن طرق التثبيت المستندة إلى الشبكة أكثر شيوعًا.

تصف إدخالات **cdrom** أقراص CD / DVD-ROM لديك. على عكس الإدخالات الأخرى، لا يتوفر القرص المضغوط دائمًا، حيث يجب إدراجه في محرك الأقراص وعادة ما يمكن قراءة قرص واحد فقط في كل مرة. لهذه الأسباب، تتم إدارة هذه المصادر بطريقة مختلفة قليلاً ويجب إضافتها باستخدام برنامج **apt-cdrom**، والذي يتم تنفيذه عادةً باستخدام معلمة **add**. سيطلب هذا الأخير بعد ذلك إدخال القرص في محرك الأقراص وسيتصفح محتوياته بحثًا عن ملفات **الحزم**. سيستخدم هذه الملفات لتحديث قاعدة البيانات الخاصة به من الحزم المتوفرة (عادةً ما تتم هذه العملية بواسطة الأمر **apt update**). بعد ذلك، ستطلب APT القرص إذا كان بحاجة إلى حزمة مخزنة عليه.

تعتمد بنية الحقل الأخير على بنية المستودع. في أبسط الحالات، يمكنك ببساطة الإشارة إلى مجلد فرعي (مع شرطة مائلة زائدة مطلوبة) للمصدر المطلوب (غالبًا ما يكون هذا "/." بسيطًا، والذي يشير إلى عدم وجود مجلد فرعي -يتم بعد ذلك حزم مباشرة عند المحدد URL). ولكن في الحالة الأكثر شيوعًا، سيتم تنظيم المستودعات مثل مرآة دبيان، مع توزيعات متعددة لكل منها مكونات

متعددة. في هذه الحالات، قم بتسمية التوزيع المختار، ثم المكونات (أو الأقسام) التي تريد تمكينها. دعونا نتوقف لحظة لتقديم هذه الأقسام.

يستخدم ديبيان وكالي ثلاثة أقسام للتمييز بين الحزم وفقًا للتراخيص التي اختارها مؤلفو كل عمل.

تحتوي **Main** على جميع الحزم التي تتوافق تمامًا مع إرشادات ديبان للبرمجيات الحرة.

يختلف الأرشيف **non-free** لأنه يحتوي على برامج لا تتوافق (بالكامل) مع هذه المبادئ ولكن يمكن مع ذلك توزيعها دون قيود.

Contrib(مساهمات) هي مجموعة من البرامج مفتوحة المصدر لا يمكن أن تعمل بدون بعض العناصر غير الحرة. قد تتضمن هذه العناصر برامج من القسم غير المجاني أو ملفات غير مجانية مثل ROMs للألعاب، BIOS لوحدات التحكم، إلخ. تتضمن المساهمة أيضًا برامج مجانية يتطلب تجميعها عناصر خاصة، مثل VirtualBox، والتي تتطلب مترجمًا غير مجاني بناء بعض ملفاتها.

الآن، دعنا نلقي نظرة على مصادر أو مستودعات حزمة Kali Linux القياسية.

٣.١.٨. مستودعات كالي

يشير ملف **sources.list** قياسي لنظام يقوم بتشغيل Kali Linux إلى مستودع واحد (**kali-rolling**) والمكونات الثلاثة المذكورة سابقًا: **main** و**contrib** و**non-free**:

```
# Main Kali repository
deb http://http.kali.org/kali kali-rolling main contrib non-free
```

دعونا نلقي نظرة على مستودعات كالي المختلفة.

١.٣.١.٨. مستودع kali-rolling

هذا هو المستودع الرئيسي للمستخدمين النهائيين. يجب أن تحتوي دائمًا على حزم قابلة للتثبيت وحديثة. يتم إدارتها من خلال أداة تدمج debian testing والحزم الخاصة بـ Kali بطريقة تضمن أن تبعيات كل حزمة يمكن تلبيتها من خلال kali-rolling. بمعنى آخر، إذا لم يكن هناك أي خطأ في نصوص الصيانة، يجب أن تكون جميع الحزم قابلة للتثبيت.

نظرًا لأن Debian Testing يتطور يوميًا، فإن kali-rolling يتطور أيضًا. يتم أيضًا تحديث الحزم الخاصة بـ Kali بانتظام حيث نراقب إصدارات المنبع لأهم الحزم.

٣.٣.١.٨. مستودع Kali-Bleeding-Edge

يحتوي هذا المستودع على حزم مبنية تلقائيًا من مستودع Git (أو Subversion) الرئيسي. الاتجاه الصعودي هو أنه يمكنك الوصول على الفور إلى أحدث الميزات وإصلاح الأخطاء بعد أقل من ٢٤ ساعة من إنشائها. تُعد هذه طريقة مثالية للتحقق مما إذا تم إصلاح خطأ أبلغت عنه للمصدر.

الجانب السلبي هو أن هذه الحزم لم يتم اختبارها أو فحصها: إذا أثرت التغييرات الأولية على الحزمة (إضافة تبعية جديدة)، فقد لا تعمل هذه الحزمة. ولهذا السبب، يتم وضع علامة على المستودع بحيث لا تقوم APT بتثبيت الحزم منه تلقائيًا، خاصة أثناء الترقية.

يمكنك تسجيل المستودع إما عن طريق تحرير **/etc/apt/sources.list** أو عن طريق إنشاء ملف جديد في مجلد **/etc/apt/sources.list.d**، والذي يتميز بترك ملف النظام **sources.list** الأصلي بدون -تغيير. في هذا المثال، نختار إنشاء ملف منفصل **/etc/apt/sources.list.d/kali-bleeding-edge.list** مثل هذا:

```
# Kali Bleeding Edge repository

deb http://http.kali.org/kali kali-bleeding-edge main contrib non-free
```

٤.٣.١.٨. مرايا Kali Linux

تشير مقتطفات **sources.list** السابقة إلى **http.kali.org**: هذا خادم يقوم بتشغيل MirrorBrain، والذي سيعيد توجيه طلبات HTTP الخاصة بك إلى مرآة رسمية قريبة منك. تراقب MirrorBrain كل مرآة للتأكد من أنها تعمل وحديثة، سيعيد توجيهك دائمًا إلى مرآة جيدة.

تصحيح أخطاء إعادة توجيه المرآة

إذا كان لديك مشكلة في المرآة (على سبيل المثال بسبب فشل **apt update**)، يمكنك استخدام **curl -sI** لمعرفة المكان الذي تتم إعادة توجيهك إليه:

```
$ curl -sI http://http.kali.org/README
HTTP/1.1 302 Found
Date: Mon, 11 Apr 2016 09:43:21 GMT
Server: Apache/2.4.10 (Debian)
X-MirrorBrain-Mirror: ftp.free.fr
X-MirrorBrain-Realm: country
Link: <http://http.kali.org/README.meta4>; rel=describedby; type="application/metalink4+xml"
Link: <http://ftp.free.fr/pub/kali/README>; rel=duplicate; pri=1; geo=fr
Link: <http://de-rien.fr/kali/README>; rel=duplicate; pri=2; geo=fr
Link: <http://ftp.halifax.rwth-aachen.de/kali/README>; rel=duplicate; pri=3; geo=de
Link: <http://ftp.belnet.be/kali/kali/README>; rel=duplicate; pri=4; geo=be
Link: <http://ftp2.nluug.nl/os/Linux/distr/kali/README>; rel=duplicate; pri=5; geo=nl
Location: http://ftp.free.fr/pub/kali/README
Content-Type: text/html; charset=iso-8859-1
```

إذا استمرت المشكلة، يمكنك تحرير **/etc/apt/sources.list** وتشفير اسم مرآة عمل أخرى معروفة بدلاً من (أو قبل) إدخال **http.kali.org**.

لدينا أيضًا نسخة ثانية من MirrorBrain: حيث يستضيف **http.kali.org** مستودعات الحزمة، ويستضيف **cdimage.kali.org** صور ISO التي تم إصدارها.

http://cdimage.kali.org

إذا كنت تريد طلب قائمة مرايا Kali Linux الرسمية، يمكنك إضافة **mirrorlist** إلى أي عنوان URL صالح يشير إلى **http.kali.org** أو **cdimage.kali.org**.

http://http.kali.org/README.mirrorlist

http://cdimage.kali.org/README.mirrorlist

هذه القوائم ليست شاملة بسبب بعض قيود MirrorBrain (أبرزها المرايا المقيدة لبعض البلدان لا تظهر في القائمة إلا إذا كنت في بلد معين). لكنها تحتوي على أفضل المرايا: يتم صيانتها بشكل جيد ولديها كميات كبيرة من عرض النطاق الترددي المتاح.

٢.٨. تفاعل الحزم الأساسية

مسلحين بفهم أساسي لـ APT، دعنا نلقي نظرة على بعض تفاعلات الحزمة الأساسية بما في ذلك تهيئة APT؛ تركيب وإزالة وتطهير الحزم؛ وترقية نظام Kali Linux. ثم دعنا نلقي نظرة على بعض أدوات APT الرسومية.

١.٢.٨. تهيئة APT

APT عبارة عن مجموعة واسعة من المشاريع والأدوات، تتضمن خططها الأصلية واجهة رسومية. من منظور العميل، يتمحور حول أداة سطر الأوامر **apt-get** وكذلك **apt**، والتي تم تطويرها لاحقًا للتغلب على عيوب التصميم لـ **apt-get**.

هناك بدائل رسومية تم تطويرها من قبل أطراف ثالثة، بما في ذلك **synaptic** و**aptitude**، والتي سنناقشها لاحقًا. نميل إلى تفضيل **apt**، الذي نستخدمه في الأمثلة التالية. ومع ذلك، سنفصل بعض الاختلافات اللغوية الرئيسية بين الأدوات عند ظهورها.

عند العمل مع APT، يجب عليك أولاً تنزيل قائمة الحزم المتوفرة حاليًا بـ **apt update**. اعتمادًا على سرعة اتصالك، قد يستغرق ذلك بعض الوقت لأن قائمة الحزم المختلفة وقائمة المصادر وملفات الترجمة قد نمت في الحجم جنبًا إلى جنب مع تطوير دبيان. بالطبع، يتم تثبيت مجموعات تثبيت الأقراص المضغوطة/أقراص DVD بسرعة أكبر، لأنها محلية على جهازك.

٢.٢.٨. تثبيت الحزم

بفضل التصميم المدروس لنظام حزم ديان، يمكنك تثبيت الحزم، مع أو بدون تبعياتها، بسهولة إلى حد ما. دعنا نلقي نظرة على تثبيت الحزمة باستخدام **dpkg** و **apt**.

١.٢.٢.٨. تثبيت الحزم باستخدام dpkg

dpkg هي الأداة الأساسية التي ستستخدمها (إما بشكل مباشر أو غير مباشر من خلال APT) عندما تحتاج إلى تثبيت حزمة. إنه أيضًا خيار التثبيت إذا كنت تعمل دون اتصال، لأنه لا يتطلب اتصال بالإنترنت. تذكر أن dpkg لن يقوم بتثبيت أي تبعيات قد تتطلبها الحزمة. لتثبيت حزمة باستخدام **dpkg**، ما عليك سوى توفير الخيار **-i** أو **--install** والمسار لـ **.deb**. هذا يعني أنك قمت مسبقًا بتنزيل (أو الحصول على طريقة أخرى) ملف **.deb** الخاص بالحزمة لتثبيته.

```
# dpkg -i man-db_2.7.0.2-5_amd64.deb
(Reading database ... 86425 files and directories
currently installed.)
Preparing to unpack man-db_2.7.0.2-5_amd64.deb ...
Unpacking man-db (2.7.0.2-5) over (2.7.0.2-4) ...
Setting up man-db (2.7.0.2-5) ...
Updating database of manual pages ...
Processing triggers for mime-support (3.58) ...
```

يمكننا أن نرى الخطوات المختلفة التي يقوم بها **dpkg** ويمكننا أن نرى في أي نقطة قد حدث أي خطأ. يقوم خيار **i-** أو **install--** بتنفيذ خطوتين تلقائيًا: يقوم بإخراج الحزمة وتشغيل البرامج النصية للتكوين. يمكنك تنفيذ هاتين الخطوتين بشكل يدوي (كما يفعل **apt** وراء الكواليس) باستخدام خيارات **unpack--** و **configure--**، على التوالي:

```
# dpkg --unpack man-db_2.7.0.2-5_amd64.deb
(Reading database ... 86425 files and directories currently installed.)
Preparing to unpack man-db_2.7.0.2-5_amd64.deb ...
Unpacking man-db (2.7.0.2-5) over (2.7.0.2-5) ...
Processing triggers for mime-support (3.58) ...
# dpkg --configure man-db
Setting up man-db (2.7.0.2-5) ...
Updating database of manual pages ...
```

لاحظ أن سطور "Processing triggers" تشير إلى التعليمات البرمجية التي يتم تنفيذها تلقائيًا كلما قامت حزمة بإضافة الملفات أو إزالتها أو تعديلها في بعض المجلدات المراقبة. على سبيل المثال، تراقب حزمة دعم mime **/usr/lib/mime/packages** وتنفذ أمر **update-mime** كلما تغير شيء ما في هذا المجلد (مثل: **/usr/lib/mime/packages/man-db** في حالة معينة من **man-db**).

في بعض الأحيان يفشل **dpkg** في تثبيت الحزمة ويعرض خطأ. ومع ذلك، يمكنك طلب **dpkg** لتجاهل هذا وإصدار تحذير فقط بخيارات **--force-*** المختلفة. سيؤدي كتابة الأمر **dpkg --force-help** إلى عرض قائمة كاملة بهذه الخيارات. على سبيل المثال، يمكنك استخدام **dpkg** لتثبيت **zsh** بالقوة:

```
$ dpkg -i --force-overwrite zsh_5.2-5+b1_amd64.deb
```

الخطأ المتكرر، الذي من المؤكد أنك ستواجهه عاجلاً أم آجلاً، هو تضارب الملف. عندما تحتوي الحزمة على ملف تم تثبيته بالفعل بواسطة حزمة أخرى، سيرفض **dpkg** تثبيته. ستظهر أنواع الرسائل التالية:

```
Unpacking libgdm (from .../libgdm_3.8.3-2_amd64.deb) ...
dpkg: error processing /var/cache/apt/archives/libgdm_3.8.3-2_amd64.deb (--unpack): trying to overwrite '/usr/bin/gdmflexiserver', which is also in package gdm3 3.4.1-9
```

في هذه الحالة، إذا كنت تعتقد أن استبدال هذا الملف لا يمثل خطرًا كبيرًا على استقرار النظام الخاص بك (هذا هو الحال غالبا)، يمكنك استخدام **--force-overwrite** لاستبدال الملف.

في حين أن هناك العديد من خيارات **--force-*** المتاحة، فمن المحتمل أن يتم استخدام **--force-overwrite** بانتظام. توجد هذه الخيارات في حالات استثنائية، ومن الأفضل تركها بمفردها قدر الإمكان من أجل احترام القواعد التي تفرضها آلية التعبئة والتغليف. لا تنس أن هذه القواعد تضمن اتساق واستقرار النظام الخاص بك.

٢.٢.٢.٨. تثبيت الحزم بـ APT

على الرغم من أن APT أكثر تقدمًا بكثير من **dpkg** وتقوم بالكثير من وراء الكواليس، ستجد أن التفاعل مع الحزم بسيط للغاية. يمكنك إضافة حزمة إلى النظام ببساطة عن طريق **apt install** *package*. ستقوم APT تلقائيًا بتثبيت التبعيات اللازمة:

```
# apt install kali-linux-gpu
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  oclgausscrack oclhashcat
The following NEW packages will be installed:
  kali-linux-gpu oclgausscrack oclhashcat
0 upgraded, 3 newly installed, 0 to remove and 416 not upgraded.
Need to get 2,494 kB of archives.
After this operation, 51.5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://archive-2.kali.org/kali kali-rolling/non-free amd64
oclhashcat amd64 2.01+git20160114-0kali2 [2,451 kB]
```

```
Get:2 http://archive-2.kali.org/kali kali-rolling/main amd64 oclgausscrack amd64 1.3-1kali2 [37.2 kB]

Get:3 http://archive-2.kali.org/kali kali-rolling/main amd64 kali-linux-gpu amd64 2016.3.2 [6,412 B]

Fetched 2,494 kB in 0s (3,060 kB/s)

Selecting previously unselected package oclhashcat.

(Reading database ... 317084 files and directories currently installed.)

Preparing to unpack .../0-oclhashcat_2.01+git20160114-0kali2_amd64.deb ...

Unpacking oclhashcat (2.01+git20160114-0kali2) ...

Selecting previously unselected package oclgausscrack.

Preparing to unpack .../1-oclgausscrack_1.3-1kali2_amd64.deb ...

Unpacking oclgausscrack (1.3-1kali2) ...

Selecting previously unselected package kali-linux-gpu.

Preparing to unpack .../2-kali-linux-gpu_2016.3.2_amd64.deb ...

Unpacking kali-linux-gpu (2016.3.2) ...

Setting up oclhashcat (2.01+git20160114-0kali2) ...

Setting up oclgausscrack (1.3-1kali2) ...

Setting up kali-linux-gpu (2016.3.2) ...
```

يمكنك أيضًا استخدام **apt-get install** *package* أو **aptitude install** *package* لتثبيت الحزم البسيطة، فإنها تفعل نفس الشيء في الأساس. كما سترى لاحقًا، فإن الاختلافات أكثر فائدة للترقيات أو عندما لا يكون لحل التبعيات أي حل مثالي.

إذا كانت **sources.list** تسرد العديد من التوزيعات، يمكنك تحديد إصدار الحزمة باستخدام *package*=*version* **apt install**، ولكن مع الإشارة إلى توزيعها الأصلي (kali-rolling أو kali-dev أو kali-bleeding-edge) بـ **apt install** *package/distribution* هو يفضل عادة.

كما هو الحال مع **dpkg**، يمكنك أيضًا توجيه **apt** لتثبيت حزمة بالقوة واستبدال الملفات باستخدام **force-overwrite--**، لكن بناء الجملة غريب بعض الشيء لأنك تمرر المدخل لـ **dpkg**:

```
# apt -o Dpkg::Options::="--force-overwrite"
install zsh
```

٣.٢.٨. ترقية kali linux

كتوزيع محدث "rolling"، يتمتع Kali Linux بقدرات ترقية مذهلة. في هذا القسم، سنلقي نظرة على مدى سهولة ترقية Kali، وسنناقش استراتيجيات تخطيط تحديثاتك.

نوصي بإجراء ترقيات منتظمة، لأنها ستقوم بتثبيت آخر تحديثات الأمان. للترقية، استخدم: **apt update** متبوعًا إما بـ **apt upgrade** أو **apt-get upgrade** أو **aptitude safe-upgrade**. تبحث هذه الأوامر عن الحزم المثبتة التي يمكن ترقيتها دون إزالة أي حزمة. بمعنى آخر، الهدف هو ضمان أقل قدر ممكن من الترقية. تعد أداة سطر

الأوامر **apt-get** أكثر تطلباً قليلاً من **aptitude** أو **apt** لأنها سترفض تثبيت الحزم التي لم يتم تثبيتها مسبقًا.

ستختار أداة **apt** بشكل عام رقم الإصدار الأحدث (باستثناء الحزم من kali-bleeding-edge، والتي يتم تجاهلها افتراضياً بغض النظر عن رقم الإصدار الخاص بها).

لإخبار **apt** باستخدام توزيع معين عند البحث عن الحزم التي تمت ترقيتها، تحتاج إلى استخدام الخيار **t-** أو **target-release--**، متبوعًا باسم التوزيعة التي تريدها (على سبيل المثال: **apt -t kali-rolling upgrade**). لتجنب اختيار هذا الخيار في كل مرة تستخدم فيها **apt**، يمكنك إضافة **APT::Default-Release "kali-rolling";** في الملف **/etc/apt/apt.conf.d/local**.

للحصول على ترقيات أكثر أهمية، مثل ترقيات الإصدارات الرئيسية، استخدم **apt full-upgrade**. باستخدام هذه التعليمات، سيكمل **apt** الترقية حتى إذا كان عليه إزالة بعض الحزم القديمة أو تثبيت تبعيات جديدة. هذا هو الأمر الذي يجب عليك استخدامه للترقيات العادية لنظام Kali Rolling الخاص بك. الأمر بسيط للغاية لدرجة أنه لا يحتاج إلى شرح: تستند سمعة APT على هذه الوظيفة الرائعة.

على عكس **apt** و **aptitude**، لا تعرف **apt-get** أمر **full-upgrade**. بدلاً من ذلك، يجب عليك استخدام **apt-get dist-Upgrade** (ترقية التوزيع)، وهو أمر معروف يقبله **apt** و **aptitude** أيضًا للتوافق مع الإصدارات السابقة.

كن على علم بالتغييرات الهامة

لاستباق بعض هذه المشاكل، يمكنك تثبيت حزمة **apt-listchanges**، التي تعرض معلومات حول المشاكل المحتملة في بداية ترقية الحزمة. يقوم مشرفو الحزم بتجميع هذه المعلومات ووضعها في ملفات **/usr/share/doc/*package*/NEWS.Debian** لصالحك. يجب أن تساعدك قراءة هذه الملفات (ربما من خلال apt-listchanges) على تجنب المفاجآت السيئة.

منذ أن أصبحت توزيعًا محدثا "rolling"، يمكن لـ Kali تلقي ترقيات عدة مرات في اليوم. ومع ذلك، قد لا تكون هذه أفضل استراتيجية. لذا، كم مرة يجب ترقية kali linux؟ لا توجد قاعدة ثابتة ولكن هناك بعض الإرشادات التي يمكن أن تساعدك. يجب عليك الترقية:

- عندما تكون على علم بمشكلة أمنية تم إصلاحها في أحد التحديثات
- عندما تشك في أن إصدارًا محدثًا قد يعمل على إصلاح خطأ تواجهه
- قبل الإبلاغ عن خطأ للتأكد من أنه لا يزال موجودًا في أحدث إصدار متوفر لديك
- غالبًا ما يكفي للحصول على إصلاحات الأمان التي لم تسمع عنها

هناك أيضًا حالات يكون من الأفضل فيها عدم الترقية. على سبيل المثال، قد لا تكون فكرة جيدة للترقية:

❖ إذا كنت لا تستطيع تحمل أي كسر (على سبيل المثال، لأنك في وضع عدم الاتصال، أو لأنك على وشك تقديم عرض تقديمي بجهازك)؛ من الأفضل إجراء الترقية لاحقًا، عندما يكون لديك الوقت الكافي لاستكشاف أي مشكلة تم تقديمها في العملية وإصلاحها.

❖ إذا حدث تغيير مزعج مؤخرًا (أو لا يزال مستمرًا) وتخشى عدم اكتشاف جميع المشكلات حتى الآن. على سبيل المثال، عندما يتم إصدار نسخة gnome جديدة، لا يتم تحديث جميع الحزم في نفس الوقت ومن المحتمل أن يكون لديك مزيج من الحزم مع الإصدار القديم والإصدار الجديد. في معظم الأحيان، هذا جيد ويساعد الجميع على إطلاق هذه التحديثات بشكل تدريجي، ولكن هناك دائمًا استثناءات وقد يتم كسر بعض التطبيقات بسبب مثل هذه التناقضات.

❖ إذا أخبرك ناتج **apt full-upgrade** أنه سيزيل الحزم التي تعتبرها مهمة لعملك. في هذه الحالات، تريد مراجعة الموقف ومحاولة فهم سبب رغبة **apt** في إزالتها. ربما تكون الحزم معطلة حاليًا وفي هذه الحالة قد ترغب في الانتظار حتى تتوفر الإصدارات الثابتة، أو قد تم تجاوزها ويجب عليك تحديد بدائلها ثم متابعة الترقية الكاملة على أي حال.

بشكل عام، نوصي بترقية kali مرة واحدة على الأقل في الأسبوع. يمكنك بالتأكيد الترقية يوميًا ولكن من غير المنطقي القيام بذلك أكثر من ذلك. حتى لو كانت المرايا متزامنة أربع مرات في اليوم، فإن التحديثات القادمة من دبيان عادة ما تنزل مرة واحدة فقط في اليوم.

٤.٢.٨. إزالة وتطهير الحزم

إزالة الحزمة أبسط من تثبيت حزمة. دعونا نلقي نظرة على كيفية إزالة حزمة باستخدام **dpkg** و**apt**.

لإزالة حزمة باستخدام **dpkg**، قم كتابة الخيار **r-** أو **remove--**، متبوعًا باسم الحزمة. ومع ذلك، هذه الإزالة ليست مكتملة: جميع ملفات التكوين، البرامج النصية لصاحب العمل، ملفات السجل (سجلات النظام)، البيانات التي تم إنشاؤها بواسطة البرنامج الخفي (مثل محتوى مجلد خادم LDAP أو محتوى قاعدة البيانات لخادم SQL)، ومعظم بيانات المستخدم الأخرى التي تتم معالجتها بواسطة الحزمة تظل كما هي. يسهّل خيار الإزالة إلغاء تثبيت برنامج وإعادة تثبيته لاحقًا بنفس التكوين. تذكر أيضًا أنه لا تتم إزالة التبعيات. تأمل هذا المثال:

```
# dpkg --remove kali-linux-gpu
(Reading database ... 317681 files and directories currently installed.)
Removing kali-linux-gpu (2016.3.2) ...
```

يمكنك أيضًا إزالة الحزم من النظام باستخدام **apt remove** *package*. ستقوم APT تلقائيًا بحذف الحزم التي تعتمد على الحزمة التي يتم إزالتها. مثل مثال **dpkg**، لن تتم إزالة ملفات التكوين وبيانات المستخدم.

من خلال إضافة اللواحق لأسماء الحزم، يمكنك استخدام **apt** (أو **apt-get** و**aptitude**) لتثبيت حزم معينة وإزالة حزم أخرى على نفس سطر الأوامر. باستخدام أمر

باستخدام الأمر **apt install**، أضف "-" لأسماء الحزم التي تريد إزالتها. باستخدام الأمر **apt remove** ، وأضف "+"لأسماء الحزم التي ترغب في تثبيتها.

يوضح المثال التالي طريقتين مختلفتين لتثبيت *package1* وإزالة *package2*.

```
# apt install package1 package2-
[...]
# apt remove package1+ package2
[...]
```

يمكن استخدام هذا أيضًا لاستبعاد الحزم التي سيتم تثبيتها بخلاف ذلك، على سبيل المثال بسبب التوصيات **"Recommends"** (ستتم مناقشتها لاحقًا). بشكل عام، سيستخدم محلول التبعية تلك المعلومات كإشارة للبحث عن حلول بديلة.

لإزالة جميع البيانات المرتبطة بالحزمة، يمكنك مسح الحزمة باستخدام **dpkg -P** *package*، أو أوامر **apt purge** *package*. سيؤدي ذلك إلى إزالة الحزمة بالكامل وجميع بيانات المستخدم، وفي حالة **apt**، سيتم حذف التبعيات أيضًا.

```
# dpkg -r debian-cd
(Reading database ... 97747 files and directories currently installed.)
Removing debian-cd (3.1.17) ...
# dpkg -P debian-cd
(Reading database ... 97401 files and directories currently installed.)
Removing debian-cd (3.1.17) ...
```

```
Purging configuration files for debian-cd (3.1.17)
...
```

تحذير! بالنظر إلى الطبيعة النهائية للتطهير، لا تنفذها باستخفاف. ستفقد كل شيء مرتبط بتلك الحزمة.

٥.٢.٨. فحص الحزم

بعد ذلك، دعونا نلقي نظرة على بعض الأدوات التي يمكن استخدامها لفحص حزم دبيان. سنتعرف على أوامر **dpkg** و**apt** و **apt-cache** التي يمكن استخدامها للاستعلام وتصور قاعدة بيانات الحزمة.

١.٥.٢.٨. الاستعلام عن قاعدة بيانات dpkg وفحص ملفات deb.

سنبدأ بالعديد من خيارات **dpkg** التي تستعلم عن قاعدة بيانات **dpkg** الداخلية. توجد قاعدة البيانات هذه في نظام الملفات في **var/lib/dpkg/** وتحتوي على أقسام متعددة بما في ذلك البرامج النصية للتكوين (**var/lib/dpkg/info/**)، وهي قائمة بالملفات التي تم تثبيت الحزمة عليها (**var/lib/dpkg/info/*.list/**)، وحالة كل حزمة تم تثبيتها (**var/lib/dpkg/status/**). يمكنك استخدام **dpkg** للتفاعل مع الملفات الموجودة في قاعدة البيانات هذه. لاحظ أن معظم الخيارات متوفرة في إصدار طويل (كلمة واحدة أو أكثر ذات صلة، مسبوقة بشرطة مزدوجة)

ونسخة قصيرة (حرف واحد، غالبًا ما يكون الحرف الأول من كلمة واحدة من النسخة الطويلة، ويسبقه شرطة واحدة). هذا الاصطلاح شائع جدًا لدرجة أنه معيار POSIX.

أولاً، دعنا نلقي نظرة على *package* **--listfiles** (أو **-L**)، والتي تسرد الملفات التي تم تثبيتها بواسطة الحزمة المحددة:

```
$ dpkg -L base-passwd
/.
/usr
/usr/sbin
/usr/sbin/update-passwd
/usr/share
/usr/share/lintian
/usr/share/lintian/overrides
/usr/share/lintian/overrides/base-passwd
/usr/share/doc-base
/usr/share/doc-base/users-and-groups
/usr/share/base-passwd
/usr/share/base-passwd/group.master
/usr/share/base-passwd/passwd.master
/usr/share/man
/usr/share/man/pl
/usr/share/man/pl/man8
/usr/share/man/pl/man8/update-passwd.8.gz
```

```
[...]
/usr/share/doc
/usr/share/doc/base-passwd
/usr/share/doc/base-passwd/users-and-groups.txt.gz
/usr/share/doc/base-passwd/changelog.gz
/usr/share/doc/base-passwd/copyright
/usr/share/doc/base-passwd/README
/usr/share/doc/base-passwd/users-and-groups.html
```

بعد ذلك، *file* **dpkg --search** (أو **S-**)، يجد أي حزم تحتوي على الملف أو المسار الذي تم تمريره كمدخل. على سبيل المثال، للعثور على الحزمة التي تحتوي على **bin/date/**:

```
$ dpkg -S /bin/date
coreutils: /bin/date
```

يعرض الأمر *package* **dpkg --status** (أو **s-**) رؤوس الحزمة المثبتة. على سبيل المثال، للبحث في الرؤوس عن حزمة **Coreutils**:

```
$ dpkg -s coreutils
Package: coreutils
Essential: yes
Status: install ok installed
Priority: required
Section: utils
Installed-Size: 13855
Maintainer: Michael Stone <mstone@debian.org>
```

```
Architecture: amd64
Multi-Arch: foreign
Version: 8.23-3
Replaces: mktemp, realpath, timeout
Pre-Depends: libacl1 (>= 2.2.51-8), libattr1 (>= 1:2.4.46-8), libc6 (>= 2.17), libselinux1 (>= 2.1.13)
Conflicts: timeout
Description: GNU core utilities
This package contains the basic file, shell and text manipulation
utilities which are expected to exist on every operating system.
.
Specifically, this package includes:
arch base64 basename cat chcon chgrp chmod chown chroot cksum comm cp
csplit cut date dd df dir dircolors dirname du echo env expand expr
factor false flock fmt fold groups head hostid id install join link ln
logname ls md5sum mkdir mkfifo mknod mktemp mv nice nl nohup nproc numfmt
od paste pathchk pinky pr printenv printf ptx pwd readlink realpath rm
rmdir runcon sha*sum seq shred sleep sort split stat stty sum sync tac
tail tee test timeout touch tr true truncate tsort tty uname unexpand
uniq unlink users vdir wc who whoami yes
Homepage: http://gnu.org/software/coreutils
```

يعرض الأمر **dpkg --list** (أو **-l**) قائمة الحزم المعروفة للنظام وحالة التثبيت الخاصة بها. يمكنك أيضًا استخدام **grep** على الإخراج للبحث عن حقول معينة، أو توفير أحرف البدل (مثل **b***) للبحث عن الحزم التي تتطابق مع سلسلة بحث جزئية معينة. سيعرض هذا ملخص الحزم. على سبيل المثال، لإظهار قائمة ملخصة لجميع الحزم التي تبدأ بالحرف "b":

```
$ dpkg -l 'b*'
Desired=Unknown/Install/Remove/Purge/Hold
|     Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
```

```
||/ Name           Version      Architecture Description
+++-================-=================-==============-
====================================
ii  b43-fwcutter   1:019-3     amd64       utility
for extracting Broadcom 4
ii  backdoor-facto 3.4.2-0kali1 all         Patch
win32/64 binaries with shel
un  backupninja                         (no description
available)
un  backuppc                            (no description
available)
ii  baobab         3.22.1-1     amd64         GNOME
disk usage analyzer
[...]
```

يسرد الأمر *file.deb* **dpkg --contents** (أو **-c**) جميع الملفات في ملف **.deb** معين:

```
$ dpkg -c /var/cache/apt/archives/gnupg_1.4.18-6_amd64.deb
drwxr-xr-x root/root         0 2014-12-04 23:03 ./
drwxr-xr-x root/root         0 2014-12-04 23:03 ./lib/
drwxr-xr-x root/root         0 2014-12-04 23:03 ./lib/udev/
drwxr-xr-x root/root         0 2014-12-04 23:03 ./lib/udev/rules.d/
-rw-r--r-- root/root      2711 2014-12-04 23:03
./lib/udev/rules.d/60-gnupg.rules
drwxr-xr-x root/root         0 2014-12-04 23:03 ./usr/
drwxr-xr-x root/root         0 2014-12-04 23:03 ./usr/lib/
```

```
drwxr-xr-x root/root        0 2014-12-04 23:03 ./usr/lib/gnupg/
-rwxr-xr-x   root/root              39328   2014-12-04   23:03
./usr/lib/gnupg/gpgkeys_ldap
-rwxr-xr-x   root/root              92872   2014-12-04   23:03
./usr/lib/gnupg/gpgkeys_hkp
-rwxr-xr-x   root/root              47576   2014-12-04   23:03
./usr/lib/gnupg/gpgkeys_finger
-rwxr-xr-x   root/root              84648   2014-12-04   23:03
./usr/lib/gnupg/gpgkeys_curl
-rwxr-xr-x   root/root               3499   2014-12-04   23:03
./usr/lib/gnupg/gpgkeys_mailto
drwxr-xr-x root/root        0 2014-12-04 23:03 ./usr/bin/
-rwxr-xr-x root/root    60128 2014-12-04 23:03 ./usr/bin/gpgsplit
-rwxr-xr-x root/root  1012688 2014-12-04 23:03 ./usr/bin/gpg
[...]
```

يعرض الأمر `dpkg --info` *file.deb* (أو `-I`) رؤوس ملف **deb**، المحدد:

```
$ dpkg -I /var/cache/apt/archives/gnupg_1.4.18-6_amd64.deb
new debian package, version 2.0.
 size 1148362 bytes: control archive=3422 bytes.
    1264 bytes,    26 lines      control
    4521 bytes,    65 lines      md5sums
     479 bytes,    13 lines   *  postinst  #!/bin/sh
     473 bytes,    13 lines   *  preinst   #!/bin/sh
 Package: gnupg
 Version: 1.4.18-6
```

```
Architecture: amd64
Maintainer: Debian GnuPG-Maintainers <pkg-gnupg-maint@lists.alioth.debian.org>
Installed-Size: 4888
Depends: gpgv, libbz2-1.0, libc6 (>= 2.15), libreadline6 (>= 6.0), libusb-0.1-4 (>= 2:0.1.12), zlib1g (>= 1:1.1.4)
Recommends: gnupg-curl, libldap-2.4-2 (>= 2.4.7)
Suggests: gnupg-doc, libpcsclite1, parcimonie, xloadimage | imagemagick | eog
Section: utils
Priority: important
Multi-Arch: foreign
Homepage: http://www.gnupg.org
Description: GNU privacy guard - a free PGP replacement
 GnuPG is GNU's tool for secure communication and data storage.
 It can be used to encrypt data and to create digital signatures.
 It includes an advanced key management facility and is compliant
 with the proposed OpenPGP Internet standard as described in RFC 4880.
[...]
```

يمكنك أيضًا استخدام **dpkg** لمقارنة أرقام إصدارات الحزمة مع خيار **--compare-versions**، والذي غالبًا ما يتم استدعاؤه بواسطة البرامج الخارجية، بما في ذلك البرامج النصية للتهيئة التي تنفذها **dpkg** نفسها. يتطلب هذا الخيار ثلاث معلمات: رقم الإصدار وعامل المقارنة ورقم الإصدار الثاني. العوامل المحتملة المختلفة هي: **lt** (أقل من ذلك تمامًا)، **le** (أقل من أو يساوي) ، **eq** (يساوي) ، **ne** (لا يساوي) ، **ge** (أكبر من أو يساوي) ، و **gt** (أكبر من). إذا كانت المقارنة صحيحة، **dpkg** ترجع 0 (النجاح)؛ إذا لم يكن كذلك، فإنه يعطي قيمة إرجاع غير صفرية (تشير إلى الفشل). فكر في هذه المقارنات:

```
$ dpkg --compare-versions 1.2-3 gt 1.1-4
$ echo $?
0
$ dpkg --compare-versions 1.2-3 lt 1.1-4
$ echo $?
1
$ dpkg --compare-versions 2.6.0pre3-1 lt 2.6.0-1
$ echo $?
1
```

لاحظ الفشل غير المتوقع في المقارنة الأخيرة: بالنسبة إلى **dpkg**، ليس للسلسلة "**pre**" (التي تشير عادةً إلى الإصدار التجريبي) معنى خاصًا، و **dpkg** يفسرها ببساطة على أنها سلسلة، وفي هذه الحالة يكون "**2.6.0pre3-1**" أبجديًا أكبر من "**2.6.0-1**". عندما نريد أن يشير رقم إصدار الحزمة إلى أنها نسخة تجريبية، فإننا نستخدم حرف التلدة، "**~**":

```
$ dpkg --compare-versions 2.6.0~pre3-1 lt 2.6.0-1
$ echo $?
0
```

٢.٥.٢.٨. الاستعلام عن قاعدة بيانات الحزم المتوفرة باستخدام apt-cache و apt

يمكن أن يعرض الأمر **apt-cache** الكثير من المعلومات المخزنة في قاعدة بيانات APT الداخلية. هذه المعلومات هي نوع من ذاكرة التخزين المؤقت حيث يتم جمعها من المصادر المختلفة المدرجة في ملف **sources.list**. يحدث هذا أثناء عملية **apt update** المناسبة.

VOCABULARY Cache

مخبأ المفردات

ذاكرة التخزين المؤقت هي نظام تخزين مؤقت يستخدم لتسريع الوصول المتكرر للبيانات عندما تكون طريقة الوصول المعتادة باهظة الثمن (من حيث الأداء). يمكن تطبيق هذا المفهوم في العديد من المواقف وبمقاييس مختلفة، من قلب المعالجات الدقيقة إلى أنظمة التخزين المتطورة.

في حالة APT، ملفات الحزم المرجعية هي تلك الموجودة على مرايا دبيان. ومع ذلك، سيكون من غير المجدي دفع كل بحث من خلال قواعد بيانات الحزمة عبر الإنترنت. هذا هو السبب في أن APT تقوم بتخزين نسخة من هذه الملفات (في **/var/lib/apt/lists/**) ويتم البحث ضمن تلك الملفات المحلية. وبالمثل، يحتوي **/var/cache/apt/archives/** على نسخة مخبأة من الحزم التي تم تنزيلها بالفعل لتجنب تنزيلها مرة أخرى إذا كنت بحاجة إلى إعادة تثبيتها.

لتجنب الاستخدام المفرط للقرص عند الترقية بشكل متكرر، يجب أن تقوم بالفرز بانتظام من خلال المجلد **/var/cache/apt/archives/**. يمكن استخدام أمرين لهذا: **apt clean** (أو **apt-get clean**) يفرغ المجلد بالكامل، يقوم **apt autoclean (apt-get autoclean)** بإزالة الحزم التي لم يعد من الممكن تنزيلها لأنها اختفت من المرآة وبالتالي فهي عديمة الفائدة. لاحظ أنه يمكن استخدام معلمة التكوين **APT::Clean-Installed** لمنع إزالة ملفات **deb.** المثبتة حاليًا. لاحظ أيضًا أن **apt** تسقط الملفات التي تم تنزيلها بمجرد تثبيتها، لذلك هذا مهم بشكل أساسي عند استخدام أدوات أخرى.

يمكن للأمر **apt-cache** إجراء عمليات بحث عن الحزم باستخدام الكلمات الأساسية بـ *keyword* **apt-cache search**. يمكنه أيضًا عرض رؤوس الإصدارات المتوفرة من الحزمة بـ *package* **apt-cache show**. يوفر هذا الأمر وصف الحزمة، وتبعياتها، واسم المشرف عليها. هذه الميزة مفيدة بشكل خاص في تحديد الحزم التي يتم تثبيتها عبر الحزم الوصفية، مثل kali-linux-wireless و kali-linux-web و kali-linux-gpu. لاحظ أن **apt search** و **apt show** و **aptitude search** و **aptitude show** تعمل بنفس الطريقة.

بديل axi-cach

يعد **apt-cache search** أداة بدائية للغاية، حيث تقوم في الأساس بتنفيذ **grep** على أوصاف الحزم. غالبًا ما تُرجع نتائج كثيرة جدًا أو لا شيء على الإطلاق، عندما يتم تضمين عدد كبير جدًا من الكلمات الرئيسية.

من ناحية أخرى، يوفر بحث *term* **axi-cache search** نتائج أفضل، مرتبة حسب الصلة. يستخدم محرك بحث *Xapian* وهو جزء من حزمة apt-xapian-index، التي تقوم بفهرسة جميع معلومات الحزمة (وأكثر من ذلك، مثل ملفات **desktop**. من جميع حزم دبيان). يعرف عن العلامات "tags" ويعيد النتائج في غضون مللي ثانية.

```
$ axi-cache search forensics graphical
5 results found.
Results 1-5:
100% autopsy - graphical interface to SleuthKit
```

```
82% forensics-colorize - show differences between files using color graphics
73% dff - Powerful, efficient and modular digital forensic framework
53% gpart - Guess PC disk partition table, find lost partitions
46% testdisk - Partition scanner and disk recovery tool, and PhotoRec file recovery tool
More terms: colorize partitions file disklabel autopsy digital differences
More tags: admin::forensics security::forensics role::program admin::recovery interface::commandline admin::boot scope::utility
```

نادرًا ما يتم استخدام بعض الميزات. على سبيل المثال، تعرض **apt-cache policy** أولويات مصادر الحزم بالإضافة إلى أولويات الحزم الفردية. مثال آخر هو **apt-cache dumpavail**، الذي يعرض رؤوس جميع الإصدارات المتاحة من جميع الحزم. يعرض **apt-cache pkgnames** قائمة بجميع الحزم التي تظهر مرة واحدة على الأقل في ذاكرة التخزين المؤقت.

٦.٢.٨. استكشاف الأخطاء وإصلاحها

عاجلاً أم آجلاً، ستواجه مشكلة عند التفاعل مع الحزمة. في هذا القسم، سنحدد بعض الخطوات الأساسية لاستكشاف الأخطاء وإصلاحها التي يمكنك اتخاذها وتوفير بعض الأدوات التي ستقودك إلى الحل المحتمل.

‎٨.٢.٦.١. معالجة المشاكل بعد الترقية

على الرغم من أفضل جهود مشرفي Kali/Debian، فإن ترقية النظام ليست دائمًا سلسة كما نأمل. قد تكون إصدارات البرامج الجديدة غير متوافقة مع الإصدارات السابقة (على سبيل المثال، قد يتغير سلوكها الافتراضي أو تنسيق بياناتها)، أو قد تنزلق الأخطاء من خلال الشقوق على الرغم من الاختبار الذي أجراه مشرفو الحزم ومستخدمي Debian Unstable.

‎٨.٢.٦.١.١. الاستفادة من تقارير الأخطاء

قد تجد أحيانًا أن إصدارًا جديدًا من البرنامج لا يعمل على الإطلاق. يحدث هذا بشكل عام إذا لم يكن التطبيق شائعًا بشكل خاص ولم يتم اختباره بما فيه الكفاية. أول شيء يجب فعله هو إلقاء نظرة على أداة تتبع أخطاء Kali ونظام تتبع الأخطاء في Debian على **https://bugs.debian.org/package** والتحقق مما إذا كانت المشكلة قد تم الإبلاغ عنها بالفعل. إذا لم يكن كذلك، فيجب عليك الإبلاغ عنها بنفسك (انظر القسم ٣.٦، "تقديم تقرير خطأ جيد" للحصول على تعليمات تفصيلية). إذا كان معروفًا بالفعل، فعادةً ما يكون تقرير الخطأ والرسائل المرتبطة به مصدرًا ممتازًا للمعلومات المتعلقة بالأخطاء. في بعض الحالات، يوجد تصحيح بالفعل وتم توفيره في تقرير الخطأ نفسه؛ يمكنك بعد ذلك إعادة ترجمة نسخة ثابتة من الحزمة المعطلة محليًا (راجع القسم ١.٩، "تعديل حزم Kali"). في حالات أخرى، ربما وجد المستخدمون حلاً للمشكلة وشاركوا أرائهم عنها في ردودهم على التقرير؛ قد تساعدك هذه التعليمات في حل المشكلة حتى يتم إصدار إصلاح أو تصحيح. في أفضل سيناريو، قد تكون الحزمة قد تم إصلاحها بالفعل وقد تجد التفاصيل في تقرير الخطأ.

٢.١.٦.٢.٨. الرجوع إلى إصدار العمل

عندما تكون المشكلة انحدارًا واضحًا (حيث يعمل الإصدار السابق)، يمكنك محاولة إرجاع الحزمة إلى إصدار سابق. في هذه الحالة، ستحتاج إلى نسخة من الإصدار القديم. إذا كان لديك حق الوصول إلى الإصدار القديم في أحد المستودعات التي تمت تهيئتها في APT، يمكنك استخدام أمر بسيط من سطر واحد للرجوع إلى إصدار أقدم (راجع القسم ٢.٢.٢.٨، "تثبيت الحزم باستخدام APT"). ولكن مع إصدار Kali's rolling، ستجد عادةً نسخة واحدة فقط من كل حزمة في المرة الواحدة.

لا يزال بإمكانك محاولة العثور على ملف **deb.** القديم وتثبيته يدويًا باستخدام **dpkg**. يمكن العثور على ملفات **deb.** القديمة في أماكن متعددة:

- ❖ في ذاكرة التخزين المؤقت لـ APT في **/var/cache/apt/archives/**
- ❖ في مجلد **pool** على مرآة كالي المعتادة (يتم الاحتفاظ بالحزم المُزالة والقديمة لمدة تتراوح من ثلاثة إلى أربعة أيام لتجنب المشاكل مع المستخدمين الذين ليس لديهم أحدث فهرس الحزمة)
- ❖ في **http://snapshot.debian.org** إذا كانت الحزمة المتأثرة مقدمة من دبيان وليس كالي، تحتفظ هذه الخدمة بالنسخ التاريخية لجميع حزم دبيان

٣.١.٦.٢.٨. التعامل مع صيانة البرامج النصية المحطمة

في بعض الأحيان يتم مقاطعة الترقية بسبب فشل أحد البرامج النصية لصاحب الحزمة (عادة ما يكون **postinst**). في هذه الحالات، يمكنك محاولة تشخيص المشكلة، وربما العمل حولها، من خلال تعديل البرنامج النصي المسبب للمشكلة.

هنا نعتمد على حقيقة أن البرمجيات النصية يتم تخزينها في **/var/lib/dpkg/info/** وأنه يمكننا مراجعتها وتعديلها.

نظراً لأن البرامج النصية لصيانة البرامج عادةً ما تكون نصوص برمجية بسيطة، فمن الممكن إضافة سطر **set -x** بعد سطر shebang وترتيبها لإعادة تشغيلها (باستخدام **dpkg --configure -a** for **postinst**) لمعرفة ما يحدث بدقة ومكان الفشل. يمكن أن يكون هذا الإخراج مكملاً جيدًا لأي تقرير خطأ قد تقدمه.

باستخدام هذه المعرفة المكتسبة حديثًا، يمكنك إما إصلاح المشكلة الأساسية أو تحويل الأمر الفاشل إلى أمر عمل (على سبيل المثال عن طريق إضافة **true** || في نهاية السطر).

لاحظ أن هذا التلميح لا يعمل في حالة فشل **preinst** حيث يتم تنفيذ هذا البرنامج النصي حتى قبل تثبيت الحزمة بحيث لا تكون في موقعها النهائي بعد. إنه يعمل من أجل **postrm** و**prerm** على الرغم من أنك ستحتاج إلى تنفيذ إزالة الحزمة (ترقية "upgrade" على التوالي) لتشغيلها.

٢.٦.٢.٨. ملف سجل dpkg

تحتفظ أداة **dpkg** بسجل لجميع إجراءاتها في **/var/log/dpkg.log**. هذا السجل مطول للغاية؛ لأنه يفصل جميع مراحل كل حزمة. بالإضافة إلى تقديم طريقة لتتبع سلوك **dpkg**، فإنه يساعد على الاحتفاظ بسجل لتطور النظام: يمكنك العثور على اللحظة الدقيقة التي تم فيها تثبيت كل حزمة أو تحديثها، ويمكن أن تكون هذه المعلومات مفيدة للغاية في فهم أحدث تغيير في السلوك. بالإضافة إلى ذلك، مع تسجيل جميع الإصدارات، من السهل التحقق من المعلومات باستخدام **changelog.Debian.gz** للحزم المعنية، أو حتى مع تقارير الأخطاء عبر الإنترنت.

```
# tail /var/log/dpkg.log
2016-12-22 09:04:05 status installed kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 startup packages remove
2016-12-22 09:20:07 status installed kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 remove kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 status half-configured kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 status half-installed kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 status config-files kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 status config-files kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 status config-files kali-linux-gpu:amd64 2016.3.2
2016-12-22 09:20:07 status not-installed kali-linux-gpu:amd64
```

٣.٦.٢.٨. إعادة تثبيت الحزم بـ apt --reinstall و aptitude reinstall

عندما تتلف نظامك عن طريق الخطأ عن طريق إزالة أو تعديل ملفات معينة، فإن أسهل طريقة لاستعادتها هي إعادة تثبيت الحزمة المتأثرة. لسوء الحظ، وجد نظام التغليف أن الحزمة مثبتة بالفعل وترفض بأدب إعادة تثبيتها. لتجنب ذلك، استخدم خيار **--reinstall** لـ **apt** وأمر **apt-get**. يعيد الأمر التالي تثبيت **postfix** حتى إذا كان موجودًا بالفعل:

```
$ apt --reinstall install postfix
```

سطر الأوامر aptitude مختلف قليلاً ولكنه يحقق نفس النتيجة بـ **aptitude reinstall postfix**. لا يمنع الأمر **dpkg** إعادة التثبيت، ولكن نادرًا ما يتم استدعاؤه مباشرة.

> **لا تستخدم apt --reinstall للتعافي من الهجوم**
>
> إن استخدام **apt --reinstall** لاستعادة الحزم التي تم تعديلها أثناء الهجوم لن يستعيد النظام بالتأكيد كما كان.
>
> بعد الهجوم، لا يمكنك الاعتماد على أي شيء: ربما تم استبدال **dpkg** و **apt** ببرامج ضارة، وليس إعادة تثبيت الملفات كما تريدها. قد يقوم المهاجم أيضًا بتعديل أو إنشاء ملفات خارجة عن سيطرة **dpkg**.

تذكر أنه يمكنك تحديد توزيع معين باستخدام **apt** أيضًا، مما يعني أنه يمكنك التراجع إلى إصدار أقدم من الحزمة (إذا كنت تعرف على سبيل المثال أنها تعمل بشكل جيد)، بشرط أن تظل متاحة في أحد المصادر المشار إليها بواسطة ملف **sources.list**:

```
# apt install w3af/kali-rolling
```

٤.٦.٢.٨. الاستفادة من *-force-- لإصلاح التبعيات المكسورة

إذا لم تكن حذرًا، فقد يؤدي استخدام خيار ***-force--** أو بعض الأعطال الأخرى إلى نظام حيث سترفض عائلة أوامر APT العمل. في الواقع، تسمح بعض هذه الخيارات بتثبيت حزمة عندما لا يتم تلبية التبعية، أو عندما يكون هناك تعارض. والنتيجة هي نظام غير متناسق من وجهة نظر التبعيات، وترفض أوامر APT تنفيذ أي إجراء باستثناء تلك التي ستعيد النظام إلى حالة متناسقة (غالبًا ما يتألف من تثبيت التبعية المفقودة أو إزالة حزمة المشكلة). ينتج عن هذا عادةً رسالة مثل هذه، يتم الحصول عليها بعد تثبيت إصدار جديد من rdesktop مع تجاهل اعتمادها على إصدار أحدث من libc6:

```
# apt full-upgrade
[...]
You might want to run 'apt-get -f install' to correct these.
The following packages have unmet dependencies:
rdesktop: Depends: libc6 (>= 2.5) but 2.3.6.ds1-13etch7 is installed
E: Unmet dependencies. Try using -f.
```

إذا كنت مشرفًا شجاعًا على يقين من صحة تحليلك، فقد تختار تجاهل التبعية أو التعارض واستخدام الخيار المقابل **--force-*‎**. في هذه الحالة، إذا كنت ترغب في الاستمرار في استخدام **apt** أو **aptitude**، يجب عليك تعديل **/var/lib/dpkg/status** لحذف أو تعديل التبعية، أو التعارض، الذي اخترت تجاوزه.

هذا التلاعب هو اختراق قبيح ويجب عدم استخدامه أبدًا، إلا في حالة الضرورة القصوى. في كثير من الأحيان، يكون الحل الأكثر ملاءمة هو إعادة تجميع الحزمة التي تسبب المشكلة أو استخدام إصدار جديد (من المحتمل تصحيحه) من مستودع يوفر backports (backports هي إصدارات أحدث خاصة معاد تجميعها للعمل في بيئة قديمة).

٧.٢.٨. الواجهات: aptitude وsynaptic

APT هو برنامج ++C الذي يوجد كوده بشكل أساسي في المكتبة المشتركة **libapt-pkg**. بفضل هذه المكتبة المشتركة، فتحت الباب لإنشاء واجهات المستخدم (الواجهات الأمامية)، حيث يمكن بسهولة إعادة استخدام كود المكتبة المشتركة. تاريخيا، تم تصميم **apt-get** فقط كواجهة أمامية اختبار لـ **libapt-pkg** لكن نجاحه يميل إلى إخفاء هذه الحقيقة.

بمرور الوقت، على الرغم من شعبية واجهات سطر الأوامر مثل **apt** و **apt-get**، تم تطوير واجهات رسومية مختلفة. سنلقي نظرة على اثنتين من تلك الواجهات في هذا القسم: **aptitude** و **synaptic**.

٨.٢.٧.١. Aptitude

Aptitude، الموضح في الشكل ١.٨، "مدير حزمة **aptitude**"، هو برنامج تفاعلي يمكن استخدامه في الوضع شبه الرسومي على وحدة التحكم. يمكنك تصفح قائمة الحزم المثبتة والمتوفرة، والبحث عن جميع المعلومات، واختيار الحزم لتثبيتها أو إزالتها. تم تصميم البرنامج خصيصًا ليستخدمه المشرفون، لذا فإن سلوكه الافتراضي أكثر ذكاءً من APT، وواجهة المستخدم أسهل بكثير في الفهم.

```
 Actions  Undo  Package  Resolver  Search  Options  Views  Help
C-T: Menu  ?: Help  q: Quit  u: Update  g: Download/Install/Remove Pkgs
aptitude 0.6.11                Will use 6,202 kB of disk spac DL Size: 2,765 kB
--\ Installed Packages (270)
  --\ admin - Administrative utilities (install software, manage users, etc) (43
    --\ main - The main Debian archive (43)
i A   acpi-support-base                                0.142-6        0.142-6
i     acpid                                            1:2.0.23-2     1:2.0.23-2
i A   adduser                                          3.113+nmu3     3.113+nmu3
i A   apt                                              1.0.9.6        1.0.9.6
i A   apt-utils                                        1.0.9.6        1.0.9.6
i     aptitude                                         0.6.11-1+b1    0.6.11-1+b1
i A   aptitude-common                                  0.6.11-1       0.6.11-1
terminal-based package manager
aptitude is a package manager with a number of useful features, including: a   #
mutt-like syntax for matching packages in a flexible manner, dselect-like
persistence of user actions, the ability to retrieve and display the Debian
changelog of most packages, and a command-line mode similar to that of apt-get.

aptitude is also Y2K-compliant, non-fattening, naturally cleansing, and
housebroken.
Homepage: http://aptitude.alioth.debian.org/


Tags: admin::configuring, admin::package-management, implemented-in::c++,
```

الشكل ١.٨، "مدير حزمة **aptitude**"

عند تشغيل **aptitude**، تظهر لك قائمة بالحزم مرتبة حسب الحالة (مثبتة أو غير مثبتة أو مثبتة ولكنها غير متاحة على المرايا)، بينما تعرض الأقسام الأخرى المهام والحزم الافتراضية والحزم الجديدة التي ظهرت مؤخرًا على المرايا. لتسهيل التصفح الموضوعي، تتوفر طرق عرض أخرى.

في جميع الحالات، يعرض **aptitude** قائمة تجمع الفئات والحزم على الشاشة. يتم تنظيم الفئات من خلال بنية شجرة، يمكن فتح فروعها أو طيها على التوالي باستخدام مفاتيح **Enter** و [, and]. يجب استخدام مفتاح + لوضع علامة على حزمة للتثبيت، - لوضع علامة عليها للإزالة، و _ لتنظيفها. لاحظ أنه يمكن أيضًا استخدام هذه المفاتيح للفئات، وفي هذه الحالة سيتم تطبيق الإجراءات المقابلة على جميع حزم الفئة. يقوم مفتاح **u** بتحديث قوائم الحزم المتوفرة ويقوم **Shift** + **u** بتحديث ترقية النظام العالمية. يتحول المفتاح **g** إلى عرض ملخص للتغييرات المطلوبة (وستؤدي كتابة **g** مرة أخرى إلى تطبيق التغييرات)، ويخرج **q** من العرض الحالي. إذا كنت في العرض الأولي، سيؤدي هذا إلى إغلاق **aptitude**.

وثائق aptitude's

لا يغطي هذا القسم التفاصيل الدقيقة لاستخدام **aptitude**، بل يركز على إعطائك مجموعة بقاء المستخدم. **aptitude** موثقة جيدًا وننصح باستخدام دليلها الكامل المتوفر في حزمة aptitude-doc-en:

/8-debian-package-management/advanced-apt-configuration-and-usage/

للبحث عن حزمة، يمكنك كتابة/متبوعًا بنمط بحث. يتطابق هذا النمط مع اسم الحزمة ولكن يمكن أيضًا تطبيقه على الوصف (إذا سبقه d~)، أو على القسم (بـ s~) ، أو على الخصائص الأخرى المفصلة في الوثائق. يمكن للنماذج نفسها تصفية قائمة الحزم المعروضة: اكتب المفتاح **l** (كما هو الحال في الحد) وأدخل النمط.

تعد إدارة العلم التلقائي لحزم دبيان (انظر القسم ٤.٣.٨، "تتبع الحزم المثبتة تلقائيًا") أمرًا سهلاً. من الممكن تصفح قائمة الحزم المثبتة ووضع علامة على الحزم على أنها آلية باستخدام **Shift + m** أو يمكنك إزالة العلامة باستخدام المفتاح **m**. يتم عرض الحزم التلقائية بحرف "**A**" في قائمة الحزم. توفر هذه الميزة أيضًا طريقة بسيطة لتصور الحزم المستخدمة على الجهاز، بدون كل المكتبات والتبعيات التي لا تهتم بها حقًا. النمط المرتبط الذي يمكن استخدامه مع l (لتنشيط وضع المرشح) هو **M~ !i~**. اختر أنك تريد فقط رؤية الحزم المثبتة (**i~**) التي لم يتم تمييزها على أنها تلقائية (**!M~**).

باستخدام aptitude على واجهة سطر الأوامر

يمكن الوصول إلى معظم ميزات **Aptitude** عبر الواجهة التفاعلية وكذلك عبر سطر الأوامر. تبدو أسطر الأوامر هذه مألوفة للمستخدمين العاديين لـ **apt-get** و **apt-cache**.

تتوفر الميزات المتقدمة في **aptitude** أيضًا في سطر الأوامر. يمكنك استخدام نفس أنماط البحث عن الحزمة كما في الإصدار التفاعلي. على سبيل المثال، إذا كنت ترغب في تنظيف قائمة الحزم المثبتة يدويًا، وإذا كنت تعلم أن أيًا من البرامج المثبتة محليًا لا تتطلب أي مكتبات معينة أو مكتبات Perl، يمكنك وضع علامة على الحزم المقابلة على أنها تلقائية باستخدام أمر واحد:

```
# aptitude markauto '~slibs|~sperl'
```

هنا، يمكنك أن ترى بوضوح قوة نظام نمط البحث من **aptitude**، والذي يتيح الاختيار الفوري لجميع الحزم في أقسام **libs** و**perl**.

احذر، إذا تم وضع علامة على بعض الحزم على أنها تلقائية وإذا لم تعتمد عليها أي حزمة أخرى، فسيتم إزالتها على الفور (بعد طلب التأكيد).

١.١.٧.٢.٨. إدارة التوصيات والاقتراحات والمهام

ميزة أخرى مثيرة للاهتمام في **aptitude** هي حقيقة أنه يحترم التوصيات بين الحزم مع الاستمرار في منح المستخدمين خيار عدم تثبيتها على أساس كل حالة على حدة. على سبيل المثال، توصي حزمة جنوم gdebi (من بين أمور أخرى). عند تحديد الأول للتثبيت، سيتم تحديد الأخير أيضًا (وسيتم وضع علامة عليه باعتباره تلقائيًا إذا لم يكن مثبتًا بالفعل على النظام).

كتابة g ستوضح: يظهر gdebi على شاشة ملخص الإجراءات المعلقة في قائمة الحزم المثبتة تلقائيًا لإرضاء التبعيات. ومع ذلك، يمكنك أن تقرر عدم تثبيته بإلغاء تحديده قبل تأكيد العمليات.

لاحظ أن ميزة تتبع التوصية هذه لا تنطبق على الترقيات. على سبيل المثال، إذا أوصى إصدار جديد من gnome بحزمة لم يوص بها سابقًا، فلن يتم وضع علامة على الحزمة للتثبيت. ومع ذلك، سيتم إدراجه في شاشة الترقية بحيث لا يزال بإمكان المسؤول تحديده للتثبيت.

تؤخذ الاقتراحات بين الحزم بعين الاعتبار أيضًا، ولكن بطريقة تتكيف مع وضعها المحدد. على سبيل المثال، نظرًا لأن gnome يقترح dia-gnome، فسيتم عرض الأخير على شاشة ملخص الإجراءات المعلقة (في قسم الحزم المقترحة بواسطة الحزم الأخرى). بهذه الطريقة، يكون مرئيًا ويمكن للمسؤول تحديد ما إذا كان سيأخذ الاقتراح في الاعتبار أم لا. نظرًا لأنه مجرد اقتراح وليس تبعية أو توصية، فلن يتم تحديد الحزمة تلقائيًا - يتطلب اختيارها تدخلًا يدويًا (وبالتالي، لن يتم وضع علامة على الحزمة على أنها تلقائية).

وبنفس السرعة، تذكر أن **aptitude** تستفيد بشكل ذكي من مفهوم المهام. نظراً لأنه يتم عرض المهام كفئات في شاشات قوائم الحزم، يمكنك إما تحديد مهمة كاملة للتثبيت أو الإزالة أو تصفح قائمة الحزم المضمنة في المهمة لتحديد مجموعة فرعية أصغر.

٢.١.٧.٢.٨. خوارزميات أفضل تفصيل

لاختتام هذا القسم، دعنا نلاحظ أن **aptitude** لديها خوارزميات أكثر تفصيلاً مقارنةً بـ **apt** عندما يتعلق الأمر بحل المواقف الصعبة. عندما يتم طلب مجموعة من الإجراءات وعندما تؤدي هذه الإجراءات المجمعة إلى نظام غير متماسك، تقيم **aptitude** العديد من السيناريوهات المحتملة وتقدمها من أجل تقليل التناقض. ومع ذلك، هذه الخوارزميات ليست مضمونة. لحسن الحظ، هناك دائمًا إمكانية تحديد الإجراءات يدويًا لتنفيذها. عندما تؤدي الإجراءات المحددة حاليًا إلى تناقضات، يشير الجزء العلوي من الشاشة إلى عدد من الحزم المكسورة (يمكنك الانتقال مباشرة إلى هذه الحزم بالضغط على **b**). ثم يمكنك إنشاء حل يدويًا. على وجه الخصوص، يمكنك الوصول إلى الإصدارات المختلفة المتاحة عن طريق تحديد الحزمة بـ **Enter**. إذا أدى تحديد أحد هذه الإصدارات إلى حل المشكلة، فلا يجب أن تتردد في استخدام الوظيفة. عندما ينخفض عدد الحزم المكسورة إلى الصفر، يمكنك الانتقال بأمان إلى شاشة ملخص الإجراءات المعلقة للتحقق الأخير قبل تطبيقها.

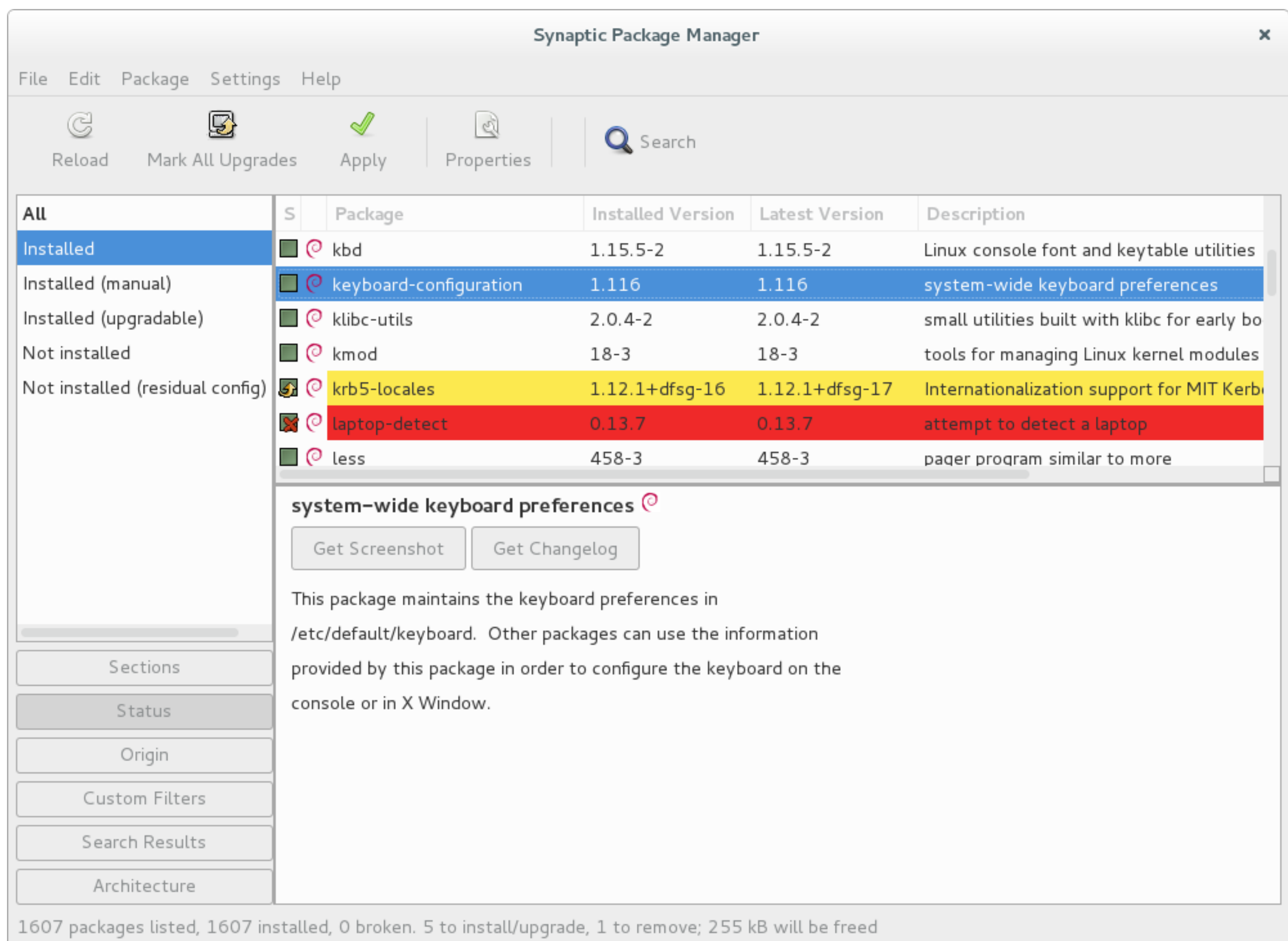
سجل aptitude

مثل **dpkg**، تحتفظ **aptitude** بتتبع الإجراءات المنفذة في ملف التسجيل الخاص بها (**/var/log/aptitude**). ومع ذلك، نظرًا لأن كلا الأمرين يعملان على مستوى مختلف تمامًا، فلا يمكنك العثور على نفس المعلومات في ملفات تسجيل الدخول الخاصة بهما. بينما تقوم سجلات **dpkg** بكافة العمليات التي يتم تنفيذها على الحزم الفردية خطوة بخطوة، فإن **aptitude** تعطي رؤية أوسع للعمليات عالية المستوى مثل الترقية على مستوى النظام.

انتبه: يحتوي ملف التسجيل هذا على ملخص للعمليات التي يتم تنفيذها بواسطة **aptitude** فقط. إذا تم استخدام واجهات أمامية أخرى (أو حتى dpkg بنفسه) من حين لآخر، فإن سجل **aptitude** سيحتوي فقط على عرض جزئي للعمليات، لذلك لا يمكنك الاعتماد عليه لبناء سجل موثوق به للنظام.

٨.٢.٧.٢. Synaptic

Synaptic هو مدير حزم رسومية يتميز بواجهة رسومية واضحة وفعالة (كما هو موضح في الشكل ٨.٢، "مدير حزم **Synaptic**") استنادًا إلى +GTK و GNOME. توفر العديد من المرشحات الجاهزة للاستخدام وصولاً سريعًا إلى الحزم المتوفرة حديثًا والحزم المثبتة والحزم القابلة للترقية والحزم القديمة وما إلى ذلك. إذا كنت تتصفح هذه القوائم، يمكنك تحديد العمليات التي يجب القيام بها على الحزم (تثبيت، ترقية، إزالة، تطهير)؛ لا يتم تنفيذ هذه العمليات على الفور، ولكن يتم وضعها في قائمة المهام. نقرة واحدة على زر ثم التحقق من صحة العمليات ويتم تنفيذها دفعة واحدة.



شكل ٢.٨ .مدير حزم "Synaptic"

٣.٨. تكوين APT المتقدم والاستخدام

حان الوقت الآن للتعمق في بعض الموضوعات الأكثر تقدمًا. أولاً، سنلقي نظرة على التكوين المتقدم لـ APT، والذي سيسمح لك بتعيين المزيد من الخيارات الدائمة التي ستطبق على أدوات APT. سنعرض بعد ذلك كيف يمكن التلاعب بأولويات الحزمة، مما يفتح الباب أمام التحديثات والترقيات المتقدمة المضبوطة بدقة. سنوضح أيضًا كيفية التعامل مع التوزيعات المتعددة بحيث يمكنك البدء في تجربة الحزم القادمة من توزيعات أخرى. بعد ذلك، سنلقي نظرة على كيفية تتبع الحزم المثبتة تلقائيًا، وهي القدرة التي تمكنك من إدارة الحزم المثبتة من خلال التبعيات. سنشرح أيضًا كيف يفتح الدعم متعدد الأقواس "multi-arch" الباب لتشغيل الحزم المصممة لمعماريات الأجهزة المختلفة. أخيرًا وليس آخرًا، سنناقش بروتوكولات التشفير والأدوات المساعدة التي ستتيح لك التحقق من صحة كل حزمة.

١.٣.٨. تكوين APT

قبل التعمق في تكوين APT، دعنا نأخذ لحظة لمناقشة آلية التهيئة لنظام دبيان. تاريخيا، تم التعامل مع التكوين عن طريق ملفات التكوين المخصصة. ومع ذلك، في أنظمة Linux الحديثة مثل Debian و Kali، أصبحت مجلدات التكوين باستخدام لاحقة **d.** أكثر استخدامًا. يمثل كل مجلد ملف تكوين مقسم إلى ملفات متعددة. وبهذا المعنى، فإن جميع الملفات الموجودة في **/etc/apt/apt.conf.d/** هي تعليمات لتكوين APT. يعالج APT الملفات بالترتيب الأبجدي، بحيث يمكن للملفات اللاحقة تعديل عناصر التكوين المحددة في الملفات السابقة.

توفر هذه البنية بعض المرونة للمسؤولين ومشرفي الحزم، مما يسمح لهم بإجراء تغييرات تكوين البرامج من خلال إضافات الملفات دون الحاجة إلى تغيير ملف موجود. هذا مفيد بشكل خاص لمشرفي الحزم لأنه يمكنهم استخدام هذا النهج لتكييف تكوين البرامج الأخرى للتأكد من أنها تتعايش تمامًا مع برامجهم، دون كسر سياسة دبيان التي تمنع تعديل ملفات التكوين للحزم الأخرى بشكل صريح. نظراً لآلية التكوين **d.**، لا يتعين عليك اتباع تعليمات تكوين الحزمة المتعددة يدويًا الموجودة عادةً في ملف **usr/share/doc/**_package_**/README.Debian/** الخاص بالحزمة، حيث يمكن أن يسقط المثبت ملفات التكوين.

احذر من ملفات التكوين التي تم إنشاؤها من مجلدات d.

في حين أن APT لديها دعم أصلي للمجلد **etc/apt/apt.conf.d/**، إلا أن هذا ليس هو الحال دائمًا. بالنسبة لبعض التطبيقات (مثل exim، على سبيل المثال)، يعد المجلد **d.** إضافة خاصة بـ Debian تُستخدم كمدخل لإنشاء ملف التكوين الأساسي الذي يستخدمه التطبيق حيويا. في هذه الحالات، توفر الحزم أمر "**update-***" (على سبيل المثال: **update-exim4.conf**) والذي سوف يربط الملفات من المجلدات **d.** ويحل محل ملف التكوين الرئيسي.في هذه الحالات، يجب ألا تقوم بتحرير ملف التكوين الرئيسي يدويًا حيث ستفقد التغييرات الخاصة بك في التنفيذ التالي لأمر **update-***، ويجب أيضًا ألا تنسى تشغيل الأمر السابق بعد تحرير ملف من مجلد **d.** (أو لن يتم استخدام التغييرات الخاصة بك).

مسلحًا بفهم آلية التكوين **d.**، دعنا نتحدث عن كيفية الاستفادة منها لتكوين APT. كما ناقشنا، يمكنك تغيير سلوك APT من خلال مدخلات سطر الأوامر لمثل **dpkg** في هذا المثال، الذي ينفذ تثبيتاً إجباريًا على تثبيت **zsh**:

```
# apt -o Dpkg::Options::="--force-overwrite" install zsh
```

من الواضح أن هذا أمر مرهق للغاية، خاصة إذا كنت تستخدم الخيارات بشكل متكرر، ولكن يمكنك أيضًا استخدام بنية تكوين مجلد **d.** لتكوين جوانب معينة من APT عن طريق إضافة توجيهات إلى ملف في المجلد **/etc/apt/apt.aptf.conf.d/**. على سبيل المثال، يمكن بسهولة إضافة هذا التوجيه (وأي تعليمات أخرى) إلى ملف في **/etc/apt/apt.conf.d/**. اسم هذا الملف تعسفي إلى حد ما، ولكن من الشائع استخدام إما **local** أو **99local**:

```
$ cat /etc/apt/apt.conf.d/99local
Dpkg::Options { "--force-overwrite"; }
```

هناك العديد من خيارات التكوين المفيدة الأخرى وبالتأكيد لا يمكننا تغطيتها جميعًا، ولكن أحد الخيارات التي سنتطرق إليها يشمل اتصال الشبكة. على سبيل المثال، إذا كان يمكنك فقط الوصول إلى الويب من خلال وكيل، فأضف سطرًا مثل **Acquire::http::proxy "http://*yourproxy*:3128"**. بالنسبة لخادم وكيل FTP، استخدم **Acquire::ftp::proxy "ftp://*yourproxy*"**.

لاكتشاف المزيد من خيارات التكوين، اقرأ صفحة الدليل apt.conf(5) باستخدام الأمر **man apt.conf** (للحصول على تفاصيل حول الصفحات اليدوية، راجع القسم ١.١.٦. "الصفحات اليدوية").

٢.٣.٨. إدارة أولويات الحزم

تعد إدارة الأولويات المرتبطة بكل مصدر حزمة أحد أهم جوانب تكوين APT. على سبيل المثال، قد ترغب في توسيع نظام Kali Rolling الخاص بك مع حزمة واحدة أو اثنتين أحدث من Debian Unstable أو Debian Testing. من الممكن تعيين أولوية لكل حزمة متاحة (يمكن أن يكون لنفس الحزمة عدة أولويات بناءً على نسختها أو التوزيع الذي يوفرها). ستؤثر هذه الأولويات على سلوك APT: لكل حزمة، ستحدد دائمًا الإصدار ذو الأولوية الأعلى (إلا إذا كان هذا الإصدار أقدم من الإصدار المثبت وأولويته أقل من 1000).

تحدد APT العديد من الأولويات الافتراضية. لكل إصدار حزمة مثبت أولوية 100. للإصدار غير المثبت أولوية 500 بشكل افتراضي ولكن يمكن أن يقفز إلى 990 إذا كان جزءًا من الإصدار المستهدف (المحدد بخيار سطر الأوامر t- أو**APT::Default-Release** تكوين الإصدار الافتراضي).

يمكنك تعديل الأولويات بإضافة إدخالات في ملف **etc/apt/preferences/** مع أسماء الحزم المتأثرة وإصدارها وأصلها وأولويتها الجديدة.

لن تقوم APT بتثبيت إصدار قديم من الحزمة (أي، الحزمة التي يكون رقم إصدارها أقل من رقم الحزمة المثبتة حاليًا) إلا عندما تكون أولويتها أعلى من 1000. ستقوم APT دائمًا بتثبيت الحزمة ذات الأولوية الأعلى التي تتبع هذا قيد. إذا كان للحزمتين نفس الأولوية، تقوم APT بتثبيت الحزمة الأحدث (رقم إصدارها هو الأعلى). إذا كانت هناك حزمتان من نفس الإصدار

لهما نفس الأولوية ولكنهما يختلفان في المحتوى الخاص بهما، تقوم APT بتثبيت الإصدار غير المثبت (تم إنشاء هذه القاعدة لتغطية حالة تحديث الحزمة دون زيادة رقم المراجعة، وهو أمر مطلوب عادةً).

بعبارات أكثر تحديدًا، لن يتم تثبيت حزمة ذات أولوية أقل من 0 مطلقًا. لن يتم تثبيت حزمة ذات أولوية تتراوح بين 0 و 100 إلا إذا لم يتم تثبيت إصدار آخر من الحزمة بالفعل. مع أولوية تتراوح بين 100 و 500، لن يتم تثبيت الحزمة إلا إذا لم يكن هناك إصدار أحدث مثبت أو متوفر في توزيع آخر. سيتم تثبيت حزمة ذات أولوية بين 501 و 990 فقط إذا لم يكن هناك إصدار أحدث مثبت أو متوفر في التوزيع المستهدف. مع أولوية بين 990 و 1000، سيتم تثبيت الحزمة إلا إذا كان الإصدار المثبت أحدث. ستؤدي الأولوية التي تزيد عن 1000 دائمًا إلى تثبيت الحزمة حتى إذا أجبرت APT على الرجوع إلى إصدار أقدم.

عندما يتحقق APT من **/etc/apt/preferences**، فإنه يأخذ في الاعتبار أولاً الإدخالات الأكثر تحديدًا (غالبًا تلك التي تحدد الحزمة المعنية)، ثم الإدخالات الأكثر عمومية (بما في ذلك على سبيل المثال جميع حزم التوزيع). في حالة وجود عدة إدخالات عامة، يتم استخدام المطابقة الأولى. تتضمن معايير الاختيار المتاحة اسم الحزمة والمصدر الذي يقدمها. يتم تحديد كل مصدر للحزمة من خلال المعلومات الواردة في ملف الإصدار " **Release**" الذي تقوم APT بتنزيله مع ملفات **Packages**. تحدد هذه الملفات الأصل، عادة "Kali" للحزم من المرايا الرسمية لـ Kali و "Debian" للحزم من المرايا الرسمية لـ Debian، ولكن يمكن أن يكون الأصل أيضًا اسم شخص أو منظمة لمستودعات الطرف الثالث. يوفر ملف الإصدار" **Release**" أيضًا اسم التوزيع مع نسخته. دعونا نلقي نظرة على تركيبتها من خلال بعض دراسات الحالة الواقعية لهذه الآلية.

أولوية Kali-Bleeding-Edge وDebian Experimental

إذا قمت بإدراج kali-bleeding-edge أو Debian Experimental في ملف **sources.list** الخاص بك، فلن يتم تثبيت الحزم المطابقة تقريبًا لأن أولوية APT الافتراضية الخاصة بها هي 1. هذه بالطبع حالة محددة، مصممة لمنع المستخدمين من تثبيت حزم bleeding edge عن طريق الخطأ. لا يمكن تثبيت الحزم إلا بكتابة **apt install** *package*/**kali-bleeding-edge**، على افتراض بالطبع أنك على دراية بالمخاطر والصداع المحتمل للحياة على الحافة. لا يزال من الممكن (على الرغم من أنه لا يوصى به) معالجة حزم kali-bleeding-edge/experimental مثل حزم التوزيعات الأخرى من خلال إعطائها أولوية 500. يتم ذلك بإدخال محدد في **/etc/apt/preferences**:

```
Package: *
Pin: release a=kali-bleeding-edge
Pin-Priority: 500
```

لنفترض أنك تريد فقط استخدام الحزم من Kali وأنك تريد فقط تثبيت حزم دبيان عند طلبها صراحة. يمكنك كتابة الإدخالات التالية في ملف **/etc/apt/preferences** (أو في أي ملف في **/etc/apt/preferences.d/**):

```
Package: *
Pin: release o=Kali
Pin-Priority: 900

Package: *
Pin: release o=Debian
Pin-Priority: -10
```

في المثالين الأخيرين، رأيت **a=kali-bleeding-edge**، الذي يحدد اسم التوزيع المحدد و **o=Kali** و **o=Debian**، اللذين يقصران النطاق على الحزم التي يكون أصلها Kali و Debian، على التوالي.

لنفترض الآن أن لديك خادمًا يحتوي على العديد من البرامج المحلية اعتمادًا على الإصدار 5.22 من Perl وأنك تريد التأكد من أن الترقيات لن تثبت إصدارًا آخر منه. يمكنك استخدام هذا الإدخال:

```
Package: perl
Pin: version 5.22*
Pin-Priority: 1001
```

الوثائق المرجعية لملف التكوين هذا متاحة في صفحة الدليل apt_preferences(5)، والتي يمكنك عرضها بـ **man apt_preferences**.

إضافة تعليقات في etc/apt/preferences/

> لا توجد صيغة رسمية للتعليقات في **etc/apt/preferences/**، ولكن يمكن توفير بعض الأوصاف النصية من خلال إضافة حقل شرح "**Explanation**" واحد أو أكثر في كل إدخال:
>
> Explanation: The package xserver-xorg-video-intel provided
>
> Explanation: in experimental can be used safely
>
> Package: xserver-xorg-video-intel
>
> Pin: release a=experimental
>
> Pin-Priority: 500

٣.٣.٨. العمل مع عدة توزيعات

بالنظر إلى أن **apt** هي أداة رائعة، فمن المحتمل أن ترغب في الغوص والبدء في تجربة الحزم القادمة من توزيعات أخرى. على سبيل المثال، بعد تثبيت نظام Kali Rolling، قد ترغب في تجربة حزمة برامج متاحة في Kali Dev، أو Debian Unstable، أو Debian Experimental دون الانحراف كثيرًا عن الحالة الأولية للنظام.

حتى إذا كنت ستواجه أحيانًا مشاكل أثناء مزج الحزم من توزيعات مختلفة، فإن **apt** يدير بشكل جيد للغاية ويحد من المخاطر بشكل فعال للغاية (بشرط أن تكون تبعيات الحزمة دقيقة). أولاً، قم بإدراج جميع التوزيعات المستخدمة في **etc/apt/sources.list/** وحدد توزيعك

المرجعي باستخدام معلمة **APT::Default-Release** (انظر القسم ٣.٢.٨، "ترقية Kali Linux").

لنفترض أن Kali Rolling هو توزيعك المرجعي ولكن Kali Dev و Debian Unstable مدرجة أيضًا في ملف **sources.list** الخاص بك. في هذه الحالة، يمكنك استخدام **`apt install`** *`package`*`/`**`unstable`** لتثبيت الحزمة من Debian Unstable. إذا فشل التثبيت بسبب بعض التبعيات غير المرضية، فدعه يحل هذه التبعيات داخل Unstable بإضافة المعلمة **t unstable-**.

في هذه الحالة، تتم الترقيات (**`upgrade`** و**`full-upgrade`**) داخل Kali Rolling باستثناء الحزم التي تم ترقيتها بالفعل إلى توزيع آخر: ستتبع هذه التحديثات التحديثات المتوفرة في التوزيعات الأخرى. سنشرح هذا السلوك بمساعدة الأولويات الافتراضية التي حددتها APT أدناه. لا تتردد في استخدام **`apt-cache policy`** (راجع "استخدام **apt-cache policy**") للتحقق من الأولويات المحددة.

يعتمد كل شيء على حقيقة أن APT تعتبر فقط الحزم ذات الإصدار الأعلى أو المتساوي من الحزمة المثبتة (على افتراض أن **etc/apt/preferences/** لم يتم استخدامها لفرض الأولويات الأعلى من 1000 لبعض الحزم).

استخدام apt-cache policy

لاكتساب فهم أفضل لآلية الأولوية، لا تتردد في تنفيذ **apt-cache policy** لعرض الأولوية الافتراضية المرتبطة بكل مصدر حزمة. يمكنك أيضًا استخدام **apt-cache policy** *package* لعرض أولويات جميع الإصدارات المتاحة لحزمة معينة.

لنفترض أنك قمت بتثبيت الإصدار ١ من الحزمة الأولى من Kali Rolling وأن الإصدار ٢ و٣ متاحان على التوالي في Kali Dev وDebian Unstable. النسخة المثبتة لها أولوية 100 لكن النسخة المتاحة في Kali Rolling (نفس الشيء) لها أولوية 990 (لأنها جزء من الإصدار المستهدف). الحزم في Kali Dev وDebian Unstable لها أولوية 500 (الأولوية الافتراضية لإصدار غير مثبت). الفائز هو النسخة ١ بأولوية 990. تبقى الحزمة في Kali Rolling.

لنأخذ مثالًا لحزمة أخرى تم تثبيت الإصدار ٢ من Kali Dev. الإصدار ١ متاح في Kali Rolling والإصدار ٣ في Debian Unstable. تم تجاهل الإصدار ١ (من الأولوية 990 - وبالتالي أقل من 1000) لأنه أقل من الإصدار المثبت. هذا يترك فقط الإصدارين ٢ و٣، كلاهما من الأولوية 500. في مواجهة هذا البديل، تختار APT الإصدار الأحدث، الإصدار من Debian Unstable. إذا كنت لا تريد ترحيل حزمة مثبتة من Kali Dev إلى Debian Unstable، يجب عليك تعيين أولوية أقل من 500 (490 على سبيل المثال) للحزم القادمة من Debian Unstable. يمكنك تعديل **/etc/apt/preferences** لهذا الغرض:

Package: *

Pin: release a=unstable

Pin-Priority: 490

٤.٣.٨. تتبع الحزم المثبتة تلقائيًا

إحدى الوظائف الأساسية لـ **apt** هي تتبع الحزم التي يتم تثبيتها فقط من خلال التبعيات. تسمى هذه الحزم تلقائيًا وغالبًا ما تشمل المكتبات.

باستخدام هذه المعلومات، عند إزالة الحزم، يمكن لمديري الحزم حساب قائمة بالحزم التلقائية التي لم تعد هناك حاجة إليها (لأنه لا توجد حزم مثبتة يدويًا اعتمادًا عليها). سوف يتخلص الأمر **apt autoremove** من هذه الحزم. لا تملك Aptitude هذا الأمر لأنه يزيلها تلقائيًا بمجرد التعرف عليها. في جميع الحالات، تعرض الأدوات رسالة واضحة تسرد الحزم المتأثرة.

من عادة وضع علامة تلقائية على أي حزمة لا تحتاجها مباشرةً حتى تتم إزالتها تلقائيًا عندما لا تكون ضرورية بعد الآن. يمكنك استخدام **apt-mark auto** *package* لوضع علامة على الحزمة المعطاة على أنها تلقائية، بينما **apt-mark manual** *package* العكس. يعمل **aptitude markauto** و **aptitude unmarkauto** بنفس الطريقة، على الرغم من أنهما يوفران المزيد من الميزات لوضع علامات على العديد من الحزم في وقت واحد (انظر القسم ١.٧.٢.٨، "Aptitude"). كما تسهل الواجهة التفاعلية القائمة على وحدة التحكم من **aptitude** مراجعة العلامة التلقائية على العديد من الحزم.

قد ترغب في معرفة سبب وجود حزمة مثبتة تلقائيًا على النظام. للحصول على هذه المعلومات من سطر الأوامر، يمكنك استخدام *package* **aptitude why** (لا تملك **apt** و **apt-get** ميزة مماثلة):

```
$ aptitude why python-debian
i   aptitude          Recommends apt-xapian-index
i A apt-xapian-index Depends    python-debian (>= 0.1.15)
```

٥.٣.٨. الفائدة من دعم البنيات المتعددة

تحتوي جميع حزم دبيان على حقل معماري " **Architecture**" في معلومات التحكم الخاصة بها. يمكن أن يحتوي هذا الحقل إما على "**all**" (للحزم المستقلة عن الهندسة المعمارية) أو اسم البنية التي يستهدفها (مثل amd64 أو armhf). في الحالة الأخيرة، بشكل افتراضي، لن يقوم **dpkg** بتثبيت الحزمة إلا إذا كانت هندستها تتوافق مع بنية المضيف كما تم إرجاعها بواسطة **dpkg --print-architecture**

يضمن هذا التقييد ألا ينتهي بك الأمر مع ثنائيات مترجمة لبناء بنية غير صحيحة. سيكون كل شيء مثاليًا باستثناء أن (بعض) أجهزة الحاسوب يمكنها تشغيل ثنائيات لبنيات متعددة، إما محليًا (يمكن لنظام amd64 تشغيل ثنائيات i386) أو من خلال المحاكيات.

١.٥.٣.٨. تمكين بنيات متعددة

يتيح دعم بنيات متعددة لـ **dpkg** للمستخدمين تحديد البنى الخارجية التي يمكن تثبيتها على النظام الحالي. يتم ذلك بسهولة باستخدام **dpkg --add-architecture**، كما في المثال التالي حيث يجب إضافة بنية i386 إلى نظام amd64 لتشغيل تطبيقات Windows باستخدام Wine. هناك بنية **dpkg --remove-architecture** لإسقاط دعم بنية خارجية، ولكن لا يمكن استخدامها إلا في حالة عدم تثبيت حزم من هذه البنية.

```
# dpkg --print-architecture
amd64
# wine
it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first.  as root, please
execute "dpkg --add-architecture i386 & apt-get
update & apt-get install wine32"
Usage: wine PROGRAM [ARGUMENTS...]   Run the specified program
       wine --help                   Display this help and exit
       wine --version                Output version information and exit
# dpkg --add-architecture i386
# dpkg --print-foreign-architectures
i386
# apt update
[...]
# apt install wine32
[...]
Setting up libwine:i386 (1.8.6-5) ...
Setting up vdpau-driver-all:i386 (1.1.1-6) ...
Setting up wine32:i386 (1.8.6-5) ...
```

```
Setting up libasound2-plugins:i386 (1.1.1-1) ...
Processing triggers for libc-bin (2.24-9)
# wine
Usage: wine PROGRAM [ARGUMENTS...]     Run the
specified program
     wine --help                     Display this
help and exit
     wine --version                  Output version
information and exit
# dpkg --remove-architecture i386
dpkg: error: cannot remove architecture 'i386'
currently in use by the database
# dpkg --print-foreign-architectures
i386
```

ستكتشف APT تلقائيًا متى تم تكوين **dpkg** لدعم البنيات الخارجية وسيبدأ تنزيل ملفات **Packages** المقابلة أثناء عملية التحديث.

يمكن بعد ذلك تثبيت الحزم الأجنبية بـ:

apt install *package*:*architecture*

استخدام ثنائيات i386 الملكية على amd64

هناك حالات استخدام متعددة للبنى المتعددة، ولكن الأكثر شيوعًا هو إمكانية تنفيذ ثنائيات 32 bit ‏(i386) على أنظمة 64 bit ‏(amd64)، على وجه الخصوص، نظرًا لأن العديد من تطبيقات الملكية الشائعة (مثل Skype) يتم توفيرها فقط في إصدارات 32 bit.

٢.٥.٣.٨. التغييرات ذات الصلة بتعدد البنى

لجعل البنى المتعددة مفيدة وقابلة للاستخدام في الواقع، يجب إعادة تجميع المكتبات ونقلها إلى مجلد خاص بالبنية بحيث يمكن تثبيت نسخ متعددة (تستهدف بنى مختلفة) جنباً إلى جنب. تحتوي هذه الحزم المحدثة على **Multi-Arch: same** حقل الرأس لإخبار نظام التعبئة والتغليف أن البنى المختلفة للحزمة يمكن تثبيتها بأمان (وأن هذه الحزم يمكن أن تلبي فقط تبعيات الحزم من نفس البنية).

```
$ dpkg -s libwine
dpkg-query: error: --status needs a valid package
name but 'libwine' is not: ambiguous package name
'libwine' with more than one installed instance


Use --help for help about querying packages.
$ dpkg -s libwine:amd64 libwine:i386 | grep ^Multi
Multi-Arch: same
Multi-Arch: same
$ dpkg -L libgcc1:amd64 |grep .so
[...]
/usr/lib/x86_64-linux-gnu/wine/libwine.so.1
$ dpkg -S /usr/share/doc/libwine/copyright
libwine:amd64,                          libwine:i386:
/usr/share/doc/libwine/copyright
```

من الجدير بالذكر أن Multi-Arch: يجب أن تحمل نفس الحزم أسماءها مع بنيتها حتى يمكن التعرف عليها بشكل لا لبس فيه. قد تشارك هذه الحزم الملفات أيضًا مع مثيلات أخرى من نفس الحزمة؛ يضمن **dpkg** أن تحتوي جميع الحزم على ملفات متطابقة من بت إلى بت عند مشاركتها. أيضًا، يجب أن يكون لجميع نسخ الحزمة نفس الإصدار، لذلك يجب ترقيتها معًا.

يقدم دعم Multi-Arch أيضًا بعض التحديات المثيرة للاهتمام في طريقة التعامل مع التبعيات. يتطلب إرضاء التبعية إما حزمة تحمل علامة Multi-Arch: خارجي أو حزمة تتطابق بنيتها مع الحزمة التي تعلن عن التبعية (في عملية حل الاعتمادية هذه، يفترض أن تكون الحزم المستقلة عن البنية بنفس بنية المضيف). يمكن أيضًا إضعاف التبعية للسماح لأي معمارية بالوفاء بها، بـ **any**:*package* بناء، لكن الحزم الخارجية لا يمكن أن تلبي مثل هذه التبعية إلا إذا تم تمييزها على أنها: **Multi-Arch: allowed**.

٦.٣.٨. التحقق من صحة الحزم

ترقيات النظام عمليات حساسة للغاية وتريد حقًا التأكد من تثبيت حزم رسمية فقط من مستودعات كالي. إذا تم اختراق مرآة Kali التي تستخدمها، فقد يحاول جهاز المخرب إضافة كود ضار إلى حزمة شرعية أخرى. يمكن لمثل هذه الحزمة، إذا تم تثبيتها، أن تفعل أي شيء صممها المخرب للقيام بما في ذلك الكشف عن كلمات المرور أو المعلومات السرية. للتحايل على هذا

الخطر، توفر Kali ختمًا مقاومًا للعبث لضمان - في وقت التثبيت - أن الحزمة تأتي بالفعل من مشرفها الرسمي ولم يتم تعديلها من قبل طرف ثالث.

يعمل الختم بسلسلة من تجزئات التشفير والتوقيع. الملف الموقع "**Release**" هو ملف الإصدار الذي قدمته مرايا kali. يحتوي على قائمة بملفات **Packages** (بما في ذلك النماذج المضغوطة، **Packages.gz** و **Packages.xz**، والإصدارات الإضافية)، بالإضافة إلى تجزئات MD5 وSHA1 و SHA256، مما يضمن عدم العبث بالملفات. تحتوي ملفات الحزم هذه على قائمة بحزم دبيان المتاحة على المرآة مع تجزئاتها، والتي تضمن بدورها عدم تغيير محتويات الحزم نفسها أيضًا.

يتم إدارة المفاتيح الموثوق بها بأمر **apt-key** الموجود في حزم **apt**، يحافظ هذا البرنامج على حلقة مفاتيح GnuPG العامة، والتي تستخدم للتحقق من التوقيعات في ملفات **Release.gpg** المتوفرة على المرايا. يمكن استخدامه لإضافة مفاتيح جديدة يدويًا (عند الحاجة إلى مرايا غير رسمية). بشكل عام، لا يلزم سوى مفاتيح Kali الرسمية. يتم تحديث هذه المفاتيح تلقائيًا بواسطة حزمة kali-archive-keyring (التي تضع الأزرار المقابلة في **/etc/apt/trusted.gpg.d**). ومع ذلك، يتطلب التثبيت الأول لهذه الحزمة تحديدًا: حتى إذا تم توقيع الحزمة مثل أي حزمة أخرى، فلا يمكن التحقق من التوقيع خارجيًا. لذلك يجب على المسؤولين الحذرين التحقق من بصمات المفاتيح المستوردة قبل الوثوق بها لتثبيت الحزم الجديدة:

```
# apt-key fingerprint
/etc/apt/trusted.gpg.d/debian-archive-jessie-automatic.gpg
-----------------------------------------------------------
pub   4096R/2B90D010 2014-11-21 [expires: 2022-11-19]
      Key fingerprint = 126C 0D24 BD8A 2942 CC7D  F8AC 7638
D044 2B90 D010
```

uid Debian Archive Automatic Signing Key (8/jessie)<ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-jessie-security-automatic.gpg

----

pub 4096R/C857C906 2014-11-21 [expires: 2022-11-19]

Key fingerprint = D211 6914 1CEC D440 F2EB 8DDA 9D6D 8F6B C857 C906

uid Debian Security Archive Automatic Signing Key (8/jessie)<ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-jessie-stable.gpg

----

pub 4096R/518E17E1 2013-08-17 [expires: 2021-08-15]

Key fingerprint = 75DD C3C4 A499 F1A1 8CB5 F3C8 CBF8 D6FD 518E 17E1

uid Jessie Stable Release Key<debian-release@lists.debian.org>

/etc/apt/trusted.gpg.d/debian-archive-squeeze-automatic.gpg

----

pub 4096R/473041FA 2010-08-27 [expires: 2018-03-05]

Key fingerprint = 9FED 2BCB DCD2 9CDF 7626 78CB AED4 B06F 4730 41FA

uid Debian Archive Automatic Signing Key (6.0/squeeze)<ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-squeeze-stable.gpg

----

pub 4096R/B98321F9 2010-08-07 [expires: 2017-08-05]

Key fingerprint = 0E4E DE2C 7F3E 1FC0 D033 800E 6448 1591 B983 21F9

uid Squeeze Stable Release Key<debian-release@lists.debian.org>

```
/etc/apt/trusted.gpg.d/debian-archive-wheezy-automatic.gpg
----------------------------------------------------------
pub   4096R/46925553 2012-04-27 [expires: 2020-04-25]
     Key fingerprint = A1BD 8E9D 78F7 FE5C 3E65  D8AF 8B48 AD62 4692 5553
uid                          Debian Archive Automatic
Signing Key (7.0/wheezy)<ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-wheezy-stable.gpg
-------------------------------------------------------
pub   4096R/65FFB764 2012-05-08 [expires: 2019-05-07]
     Key fingerprint = ED6D 6527 1AAC F0FF 15D1  2303 6FB2 A1C2 65FF B764
uid                 Wheezy Stable Release Key<debian-
release@lists.debian.org>
/etc/apt/trusted.gpg.d/kali-archive-keyring.gpg
-----------------------------------------------
pub   4096R/7D8D0BF6 2012-03-05 [expires: 2018-02-02]
     Key fingerprint = 44C6 513A 8E4F B3D3 0875  F758 ED44 4FF0 7D8D 0BF6
uid                  Kali Linux Repository<devel@kali.org>
sub   4096R/FC0D0DCB 2012-03-05 [expires: 2018-02-02]
```

عند إضافة مصدر حزمة تابع لجهة خارجية إلى ملف sources.list، يجب إخبار APT بالثقة بمفتاح مصادقة GPG المقابل (وإلا فسيظل يشكو من أنه لا يمكنه ضمان صحة الحزم القادمة من هذا المستودع) . الخطوة الأولى هي بالطبع الحصول على المفتاح العام. في أغلب الأحيان، سيتم توفير المفتاح كملف نصي صغير، والذي سوف نسميه key.asc في الأمثلة التالية.

لإضافة المفتاح إلى keyring الموثوق به، يمكن للمسؤول تشغيل **apt-key add <key.asc**. طريقة أخرى هي استخدام **synaptic** للواجهة الرسومية: توفر علامة التبويب المصادقة في قائمة **Settings → Repositories** القدرة على استيراد مفتاح من ملف **key.asc**.

بالنسبة للأشخاص الذين يفضلون تطبيقًا مخصصًا والمزيد من التفاصيل حول المفاتيح الموثوقة، من الممكن استخدام مفتاح **gui-apt-key** (في الحزمة التي تحمل الاسم نفسه)، وهي واجهة مستخدم رسومية صغيرة تدير المفاتيح الموثوقة.

بمجرد وجود المفاتيح المناسبة في حلقة المفاتيح "keyring"، ستتحقق APT من التوقيعات قبل أي عملية محفوفة بالمخاطر، بحيث تعرض الواجهات الأمامية تحذيرًا إذا طُلب منك تثبيت حزمة لا يمكن التحقق من صحتها.

٤.٨. مرجع حزمة APT: التعمق أكثر في نظام حزم دبيان

حان الوقت الآن للتعمق في نظام حزم دبيان وكالي. في هذه المرحلة، سوف نتجاوز الأدوات والبناء ونركز أكثر على nuts و bolts لنظام التعبئة والتغليف. ستساعدك طريقة العرض من وراء الكواليس هذه على فهم كيفية عمل APT في أساسها وستمنحك نظرة ثاقبة حول كيفية تبسيط نظام Kali وتخصيصه بجدية. لا يجوز لك بالضرورة حفظ جميع المواد في هذا القسم، ولكن المواد التفصيلية والمرجعية سوف تخدمك جيدًا أثناء نموك في إتقان نظام Kali Linux.

لقد تفاعلت حتى الآن مع بيانات حزمة APT من خلال الأدوات المتنوعة المصممة للتفاعل معها. بعد ذلك، سوف نتعمق أكثر ونلقي نظرة داخل الحزم ونلقي نظرة على المعلومات الوصفية الداخلية (أو معلومات حول المعلومات الأخرى) التي تستخدمها أدوات إدارة الحزم.

هذا المزيج من أرشيف الملفات والمعلومات الوصفية يمكن رؤيته مباشرة في بنية ملف **.deb**، وهو ببساطة عبارة عن أرشيف **ar** يربط ثلاثة ملفات:

```
$ ar t /var/cache/apt/archives/apt_1.4~beta1_amd64.deb
debian-binary
control.tar.gz
data.tar.xz
```

يحتوي ملف **debian-binary** على رقم إصدار واحد يصف تنسيق الأرشيف:

```
$ ar p /var/cache/apt/archives/apt_1.4~beta1_amd64.deb debian-binary
2.0
```

يحتوي أرشيف **control.tar.gz** على معلومات وصفية:

```
$ ar p /var/cache/apt/archives/apt_1.4~beta1_amd64.deb control.tar.gz | tar -tzf -
./
./conffiles
./control
./md5sums
./postinst
./postrm
./preinst
./prerm
./shlibs
./triggers
```

وأخيرًا، يحتوي أرشيف **data.tar.xz** (قد يختلف تنسيق الضغط) على الملفات الفعلية التي سيتم تثبيتها على نظام الملفات:

```
$ ar p /var/cache/apt/archives/apt_1.4~beta1_amd64.deb data.tar.xz | tar -tJf -
./
./etc/
./etc/apt/
./etc/apt/apt.conf.d/
./etc/apt/apt.conf.d/01autoremove
./etc/apt/preferences.d/
./etc/apt/sources.list.d/
./etc/apt/trusted.gpg.d/
./etc/cron.daily/
```

```
./etc/cron.daily/apt-compat
./etc/kernel/
./etc/kernel/postinst.d/
./etc/kernel/postinst.d/apt-auto-removal
./etc/logrotate.d/
./etc/logrotate.d/apt
./lib/
./lib/systemd/
[...]
```

لاحظ أنه في هذا المثال، أنت تعرض حزمة **deb.** في ذاكرة التخزين المؤقت لأرشيف APT وأن الأرشيف قد يحتوي على ملفات بأرقام إصدارات مختلفة عن تلك المعروضة.

في هذا القسم، سوف نقدم هذه المعلومات الوصفية الموجودة في كل حزمة ونوضح لك كيفية الاستفادة منها.

١.٤.٨. ملف التحكم

سنبدأ بالنظر في ملف التحكم " **control**" الموجود في أرشيف **control.tar.gz**. يحتوي ملف التحكم على المعلومات الأكثر حيوية حول الحزمة. يستخدم هيكلًا مشابهًا لرؤوس البريد الإلكتروني ويمكن مشاهدته باستخدام الأمر **dpkg -I**. على سبيل المثال، يبدو ملف التحكم الخاص بـ **apt** كما يلي:

```
$ dpkg -I apt_1.4~beta1_amd64.deb control
Package: apt
Version: 1.4~beta1
```

Architecture: amd64

Maintainer: APT Development Team<deity@lists.debian.org>

Installed-Size: 3478

Depends: adduser, gpgv | gpgv2 | gpgv1, debian-archive-keyring, init-system-helpers (>= 1.18~), libapt-pkg5.0 (>= 1.3~rc2), libc6 (>= 2.15), libgcc1 (>= 1:3.0), libstdc++6 (>= 5.2)

Recommends: gnupg | gnupg2 | gnupg1

Suggests: apt-doc, aptitude | synaptic | wajig, dpkg-dev (>= 1.17.2), powermgmt-base, python-apt

Breaks: apt-utils (<< 1.3~exp2~)

Replaces: apt-utils (<< 1.3~exp2~)

Section: admin

Priority: important

Description: commandline package manager

This package provides commandline tools for searching and

managing as well as querying information about packages

as a low-level access to all features of the libapt-pkg library.

.

These include:

* apt-get for retrieval of packages and information about them

from authenticated sources and for installation, upgrade and

removal of packages together with their dependencies

* apt-cache for querying available information about installed

as well as installable packages

* apt-cdrom to use removable media as a source for packages

* apt-config as an interface to the configuration settings

* apt-key as an interface to manage authentication keys

في هذا القسم، سنوجهك عبر ملف التحكم وشرح المجالات المختلفة. ستمنحك كل واحدة من هذه العناصر فهماً أفضل لنظام التعبئة والتغليف، وتمنحك المزيد من التحكم في التهيئة المضبوطة بدقة، وتوفر لك المعرفة اللازمة لاستكشاف المشكلات التي قد تحدث وإصلاحها.

٨.٤.١.١. التبعيات: حقل الـ Depends

يتم تعريف تبعيات الحزمة في حقل **Depends** في رأس الحزمة. هذه قائمة بالشروط التي يجب استيفاؤها لكي تعمل الحزمة بشكل صحيح — يتم استخدام هذه المعلومات بواسطة أدوات مثل **`apt`** من أجل تثبيت المكتبات المطلوبة، في الإصدارات المناسبة التي تحقق تبعيات الحزمة المراد تثبيتها. لكل تبعية، يمكنك تقييد نطاق الإصدارات التي تلبي هذا الشرط. وبعبارة أخرى، من الممكن التعبير عن حقيقة أنك بحاجة إلى الحزمة libc6 في إصدار يساوي أو أكبر من "٢.١٥" (مكتوب **libc6 (>= 2.15)**). عوامل مقارنة الإصدارات هي كما يلي:

أقل من: <<

أقل من أو يساوي: <=

يساوي (لاحظ أن ٢,٦,١ لا يساوي ٢,٦,١-٢): =

أكبر من أو يساوي: >=

أكبر من: >>.

في قائمة الشروط التي يجب استيفاؤها، تعمل الفاصلة كفاصل، وتفسر على أنها "AND" منطقية. في الظروف، يعبر الشريط العمودي ("|") عن "OR" المنطقي (وهو عبارة عن "OR" غير حصري "إما/أو"). يحمل أولوية أكبر من "AND"، يمكنك استخدامه عدة مرات حسب الضرورة. وبالتالي، تتم كتابة التبعية "(A OR B) وC" مكتوب **A | B, C** في المقابل، يجب كتابة "A OR (B AND C)" كـ "(A OR B) AND (A OR C)"، حيث لا يتسامح الحقل **Depends** بين الأقواس التي تغير ترتيب الأولويات بين العوامل المنطقية "OR" و "AND". وبذلك تتم كتابتها **C | A ,B | A**. راجع http://www.debian.org/doc/debian-policy/ch-relationships.html لمزيد من المعلومات.

نظام التبعيات "**Depends**" هو آلية جيدة لضمان تشغيل البرنامج ولكن له استخدام آخر مع الحزم التعريفية. هذه حزم فارغة تصف فقط التبعيات. إنها تسهل تركيب مجموعة متسقة من البرامج التي تم اختيارها مسبقًا من قبل مشرف الحزمة التعريفية؛ على هذا النحو، سيقوم **apt install** *meta-package* تلقائيًا بتثبيت جميع هذه البرامج باستخدام تبعيات الحزمة التعريفية. تعتبر حزم gnome و kde-full و kali-linux-full أمثلة على الحزم التعريفية "meta-packages".

٨.٤.١.٢. Pre-Depends، أكثر طلب من Depends

التبعيات المسبقة، المدرجة في حقل Pre-Depends في رؤوس الحزم، تكمل التبعيات العادية؛ قواعدهم متطابقة. تشير التبعية العادية إلى أنه يجب تفكيك الحزمة المعنية وتكوينها قبل تكوين الحزمة التي تعلن عن التبعية. تشترط التبعية المسبقة أنه يجب فك الحزمة المعنية وتهيئتها قبل تنفيذ البرنامج النصي للتثبيت المسبق للحزمة التي تعلن عن التبعية المسبقة، أي قبل تثبيتها.

تعتمد التبيعية المسبقة جدًا على **apt**، لأنه يضيف قيودًا صارمة على ترتيب الحزم لتثبيتها. على هذا النحو، يتم تثبيط التبعيات ما لم يكن ضروريًا للغاية. يوصى حتى باستشارة مطورين آخرين على **debian-devel@lists.debian.org** قبل إضافة تبعية مسبقة حيث من الممكن بشكل عام إيجاد حل آخر كحل بديل.

٣.١.٤.٨. حقول Recommends، Suggests، Enhances

يصف حقلي التوصيات "**Recommends**" والاقتراحات "**Suggests**" التبعيات غير الإلزامية. إن التبعيات الموصى بها، والأكثر أهمية، تحسن بشكل كبير الوظائف التي تقدمها الحزمة ولكنها ليست ضرورية لتشغيلها. تشير التبعيات المقترحة، ذات الأهمية الثانوية، إلى أن بعض الحزم قد تكمل وتزيد من فائدتها، ولكن من المعقول تمامًا تثبيت واحدة دون الأخرى.

يجب عليك دائمًا تثبيت الحزم الموصى بها إلا إذا كنت تعرف بالضبط لماذا لا تحتاجها. على العكس من ذلك، ليس من الضروري تثبيت الحزم المقترحة إلا إذا كنت تعرف سبب حاجتك إليها.

يصف حقل التحسينات "**Enhances**" أيضًا اقتراحًا، ولكن في سياق مختلف. إنه موجود بالفعل في الحزمة المقترحة، وليس في الحزمة التي تستفيد من الاقتراح. يكمن اهتمامها في أنه من الممكن إضافة اقتراح دون الحاجة إلى تعديل الحزمة المعنية. وبالتالي، يمكن أن تظهر جميع الوظائف الإضافية، والمكونات الإضافية، والامتدادات الأخرى للبرنامج في قائمة الاقتراحات المتعلقة بالبرنامج. على الرغم من وجوده منذ عدة سنوات، إلا أن هذا الحقل الأخير لا يزال يتم تجاهله إلى حد كبير من قبل برامج مثل **apt** أو **synaptic**. كان الهدف الأصلي هو السماح لحزمة

مثل **xul-ext-adblock-plus** (ملحق Firefox) بإعلان **Enhances: firefox, firefox-esr** وبالتالي تظهر في قائمة الحزم المقترحة المرتبطة بـ Firefox و Firefox-esr.

٤.١.٤.٨. التعارضات: حقل Conflicts

يشير حقل التعارضات "**Conflicts**" إلى الوقت الذي يتعذر فيه تثبيت الحزمة في وقت واحد مع حزمة أخرى. الأسباب الأكثر شيوعًا لذلك هي أن الحزمتين تتضمنان ملفًا يحمل نفس الاسم، أو يقدمان نفس الخدمة على نفس منفذ بروتوكول التحكم في الإرسال (TCP)، أو يعيقان تشغيل بعضهما البعض.

إذا تسببت في حدوث تعارض مع حزمة مثبتة بالفعل، فسوف ترفض **dpkg** تثبيت الحزمة، إلا إذا كانت الحزمة الجديدة تحدد أنها ستستبدل الحزمة المثبتة، وفي هذه الحالة ستختار **dpkg** استبدال الحزمة القديمة بالحزمة الجديدة. تتبع APT دائمًا التعليمات الخاصة بك: إذا اخترت تثبيت حزمة جديدة، فستعرض تلقائيًا إلغاء تثبيت الحزمة التي تثير مشكلة.

٥.١.٤.٨. عدم التوافق: حقل Breaks

يكون لحقل الكسر "**Breaks**" تأثير مشابه لتأثيرات حقل التعارض "**Conflicts** "، ولكن بمعنى خاص. يشير إلى أن تثبيت حزمة سيكسر حزمة أخرى (أو إصدارات معينة منها). بشكل

عام، يعد هذا التعارض بين حزمتين مؤقتاً وتشير علاقة **Breaks** على وجه التحديد إلى الإصدارات غير المتوافقة.

عندما تكسر الحزمة حزمة مثبتة بالفعل، سيرفض **`dpkg`** تثبيتها، وسيحاول **`apt`** حل المشكلة عن طريق تحديث الحزمة التي سيتم تحطيمها إلى إصدار أحدث (والذي يفترض أنه تم إصلاحه، وبالتالي، تتوافق مرة أخرى).

قد يحدث هذا النوع من المواقف في حالة التحديثات بدون توافق عكسي: هذا هو الحال إذا لم يعد الإصدار الجديد يعمل مع الإصدار الأقدم وتسبب عطلًا في برنامج آخر دون إجراء أحكام خاصة. يساعد حقل **Breaks** على منع هذه الأنواع من المشاكل.

٦.١.٤.٨. العناصر المقدمة: حقل التزويد "Provides"

يقدم هذا المجال المفهوم المثير للاهتمام للغاية *لحزمة افتراضية "virtual package"*. لها العديد من الأدوار، ولكن اثنان لهما أهمية خاصة. يتمثل الدور الأول في استخدام حزمة افتراضية لربط خدمة عامة بها (توفر الحزمة الخدمة). يشير الثاني: إلى أن الحزمة تحل محل أخرى تمامًا وأنه لهذا الغرض، يمكنها أيضًا إرضاء التبعيات التي ستفي بها الأخرى. وبالتالي من الممكن إنشاء حزمة استبدال دون الحاجة إلى استخدام نفس اسم الحزمة.

الحزم التعريفية والحزم الافتراضية

Meta-Package and Virtual Package

من الضروري التمييز بوضوح بين الحزم التعريفية والحزم الافتراضية. الأولى هي حزم حقيقية (بما في ذلك ملفات **deb.** حقيقية)، هدفها الوحيد هو التعبير عن التبعيات.

.

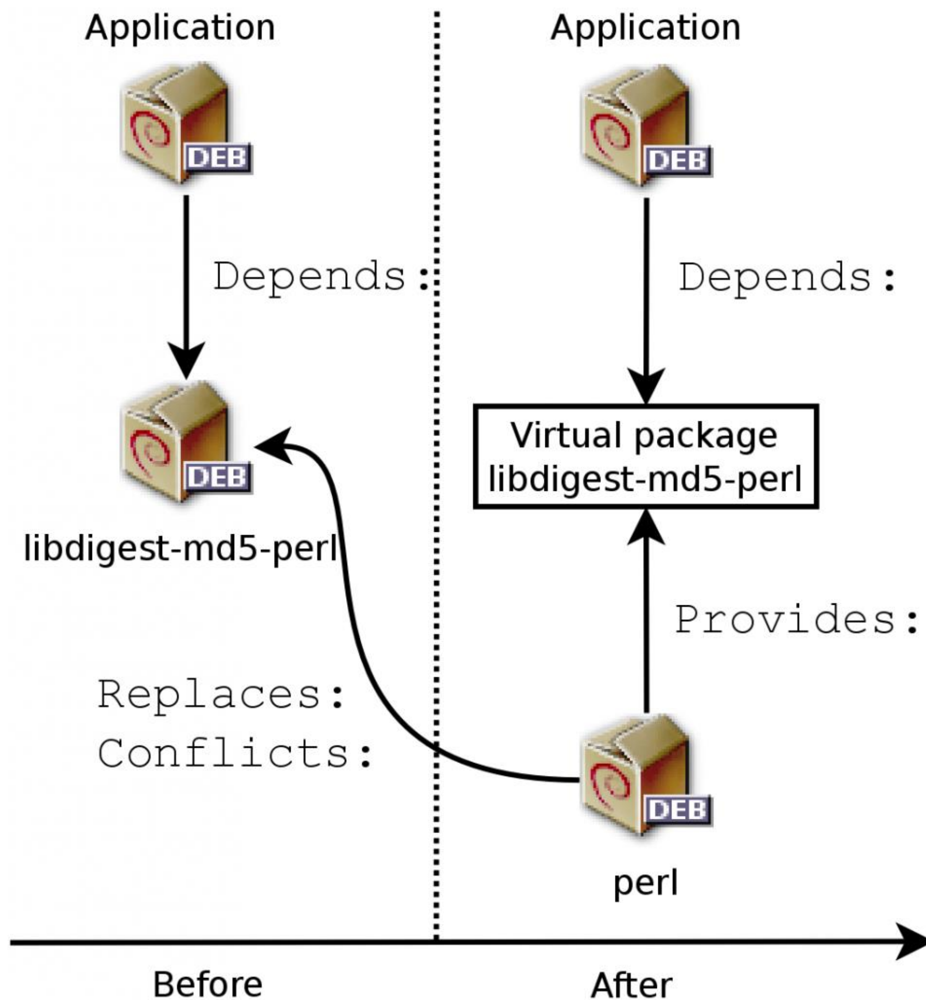
الحزم الافتراضية، لا توجد فعليا. إنها مجرد وسيلة لتحديد الحزم الحقيقية بناءً على معايير منطقية مشتركة (على سبيل المثال، الخدمة المقدمة "Providing a Service"، أو التوافق مع برنامج قياسي أو حزمة موجودة مسبقًا).

٨.٤.١.٦.١. تقديم خدمة "Providing a Service"

دعونا نناقش الحالة الأولى بمزيد من التفصيل بمثال: جميع خوادم البريد، مثل postfix أو mailmail يقال إنها توفر الحزمة الافتراضية لعامل نقل البريد. وبالتالي، فإن أي حزمة تحتاج إلى أن تكون هذه الخدمة فعالة (على سبيل المثال، مدير قائمة بريدية، مثل: smartlist أو sympa) تنص ببساطة في تبعياتها على أنها تتطلب وكيل نقل بريد بدلاً من تحديد قائمة كبيرة ولكنها غير مكتملة للحلول الممكنة. علاوة على ذلك، من غير المجدي تثبيت خادمي بريد على نفس الجهاز، ولهذا السبب تعلن كل واحدة من هذه الحزم وجود تعارض مع الحزمة الافتراضية لعامل نقل البريد. يتجاهل النظام التعارض بين الحزمة ونفسها، ولكن هذه التقنية ستحظر تثبيت خادمي بريد جنبًا إلى جنب.

٢.٦.١.٤.٨. التبادلية مع حزمة أخرى

يعتبر حقل **Provides** مثيرًا للاهتمام أيضًا عندما يتم تضمين محتوى الحزمة في حزمة أكبر. على سبيل المثال، كانت وحدة Perl libdigest-md5-perl وحدة اختيارية في Perl 5.6، وتم دمجها كمعيار قياسي في Perl 5.8. على هذا النحو، تحتوي الحزمة perl منذ الإصدار ٥.٨ المعلن على أنه يوفر **"Provides": libdigest-md5-perl** أنه يتم استيفاء التبعيات على هذه الحزمة إذا كان النظام يحتوي على Perl 5.8 (أو أحدث). تم حذف libdigest-md5-perlpackage نفسها، حيث لم يعد لها أي غرض عند إزالة إصدارات perl القديمة.



شكل ٣.٨. استخدام حقل Provides من أجل عدم كسر التبعيات

هذه الميزة مفيدة للغاية، لأنه لا يمكن أبدًا توقع تقلبات التطوير ومن الضروري أن تكون قادرًا على التكيف مع إعادة التسمية، والاستبدال التلقائي الآخر، للبرامج القديمة.

٨.٤.١.٧. استبدال الملفات: حقل الاستبدال "Replaces"

يشير حقل الاستبدال إلى أن الحزمة تحتوي على ملفات موجودة أيضًا في حزمة أخرى، ولكن يحق للحزمة استبدالها بشكل شرعي. بدون هذه المواصفات، يفشل **dpkg**، مشيرًا إلى أنه لا يمكن الكتابة فوق ملفات حزمة أخرى (من الناحية الفنية، من الممكن إجبارها على القيام بذلك باستخدام خيار **force-overwrite--**، ولكن هذا لا يعتبر عملية قياسية). هذا يسمح بتحديد المشاكل المحتملة ويتطلب من المشرف دراسة الأمر قبل اختيار ما إذا كان سيتم إضافة مثل هذا الحقل.

يتم تبرير استخدام هذا الحقل عندما تتغير أسماء الحزمة أو عندما يتم تضمين حزمة في أخرى. يحدث هذا أيضًا عندما يقرر المشرف توزيع الملفات بشكل مختلف بين الحزم الثنائية المختلفة المنتجة من نفس الحزمة المصدر: لم يعد الملف المستبدل ينتمي إلى الحزمة القديمة، ولكن فقط إلى الحزمة الجديدة.

إذا تم استبدال جميع الملفات الموجودة في حزمة مثبتة، فسيتم إزالة الحزمة. وأخيرًا، يشجع هذا الحقل أيضًا **dpkg** على إزالة الحزمة المستبدلة حيث يوجد تعارض.

٢.٤.٨. تكوين البرامج النصية

بالإضافة إلى ملف التحكم "**control**"، قد يحتوي أرشيف **control.tar.gz** على كل حزمة من حزم ديبان على عدد من النصوص البرمجية (**postinst**، **postrm**، **preinst**، **prerm**) تسمى بواسطة **dpkg** في مراحل مختلفة من معالجة الحزمة. يمكننا استخدام **dpkg -I** لإظهار هذه الملفات على أنها موجودة في أرشيف حزمة **deb**.:

```
$ dpkg -I /var/cache/apt/archives/zsh_5.3-1_amd64.deb | head
 new debian package, version 2.0.
 size 814486 bytes: control archive=2557 bytes.
     838 bytes,    20 lines      control
    3327 bytes,    43 lines      md5sums
     969  bytes,       41  lines      *    postinst
#!/bin/sh
     348  bytes,        20  lines      *     postrm
#!/bin/sh
     175  bytes,         5  lines      *    preinst
#!/bin/sh
     175  bytes,          5  lines      *     prerm
#!/bin/sh
 Package: zsh
 Version: 5.3-1
$ dpkg -I zsh_5.3-1_amd64.deb preinst
#!/bin/sh
set -e
```

```
# Automatically added by dh_installdeb
dpkg-maintscript-helper symlink_to_dir
/usr/share/doc/zsh zsh-common 5.0.7-3 -- "$@"
# End automatically added section
```

تصف سياسة دبيان كل ملف من هذه الملفات بالتفصيل، مع تحديد البرامج النصية التي تم استدعاؤها والحجج التي تتلقاها. قد تكون هذه التسلسلات معقدة، لأنه في حالة فشل أحد البرامج النصية، سيحاول **dpkg** العودة إلى حالة مرضية عن طريق إلغاء التثبيت أو الإزالة قيد التقدم (بقدر الإمكان).

قاعدة بيانات dpkg

يمكنك الوصول لقاعدة بيانات **dpkg** في نظام الملفات في **/var/lib/dpkg/**. يحتوي هذا المجلد على سجل تشغيل لجميع الحزم التي تم تثبيتها على النظام. يتم تخزين جميع سكربتات التكوين للحزم المثبتة في مجلد **/var/lib/dpkg/info/** في شكل ملف مسبوق باسم الحزمة:

```
$ ls /var/lib/dpkg/info/zsh.*
/var/lib/dpkg/info/zsh.list
/var/lib/dpkg/info/zsh.md5sums
/var/lib/dpkg/info/zsh.postinst
/var/lib/dpkg/info/zsh.postrm
/var/lib/dpkg/info/zsh.preinst
/var/lib/dpkg/info/zsh.prerm
```

يتضمن هذا المجلد أيضًا ملفًا بامتداد **list**، لكل حزمة، يحتوي على قائمة الملفات التي تنتمي إلى هذه الحزمة:

```
$ head /var/lib/dpkg/info/zsh.list
/.
/bin
/bin/zsh
/bin/zsh5
/usr
/usr/lib
/usr/lib/x86_64-linux-gnu
/usr/lib/x86_64-linux-gnu/zsh
/usr/lib/x86_64-linux-gnu/zsh/5.2
/usr/lib/x86_64-linux-gnu/zsh/5.2/zsh
[...]
```

يحتوي ملف **/var/lib/dpkg/status** على سلسلة من كتل البيانات (بتنسيق طلب رؤوس البريد الشهير للتعليق، RFC 2822) الذي يصف حالة كل حزمة. كما يتم نسخ المعلومات من ملف التحكم "control" الخاص بالحزم المثبتة هناك.

```
$ more /var/lib/dpkg/status
Package: gnome-characters
Status: install ok installed
Priority: optional
Section: gnome
Installed-Size: 1785
Maintainer: Debian GNOME Maintainers<pkg-gnome-maintainers@lists.alioth.debian.org>
Architecture: amd64
Version: 3.20.1-1
[...]
```

دعونا نناقش ملفات التكوين ونرى كيف تتفاعل. بشكل عام، يتم تنفيذ البرنامج النصي **preinst** قبل تثبيت الحزمة، بينما يتبعه **postinst**. وبالمثل، يتم استدعاء **prerm** قبل إزالة الحزمة و**postrm** بعد ذلك. تحديث الحزمة يعادل إزالة الإصدار السابق وتثبيت الإصدار الجديد. لا يمكن وصف جميع السيناريوهات المحتملة هنا بالتفصيل، ولكننا سنناقش أكثر السيناريوهات شيوعًا: التثبيت/التحديث والإزالة.

يمكن أن تكون هذه التسلسلات مربكة للغاية، ولكن قد يساعد التمثيل البصري. قام Manoj Srivastava بعمل هذه المخططات موضحا كيف يتم استدعاء البرامج النصية للتكوين بواسطة **dpkg**. كما تم تطوير مخططات مماثلة من قبل مشروع ديبان للمرأة. تكون أبسط قليلاً في الفهم، ولكنها أقل اكتمالاً.

https://people.debian.org/~srivasta/MaintainerScripts.html

https://wiki.debian.org/MaintainerScripts

تنبيه: الأسماء الرمزية للبرامج النصية

تسلسل الموصوفة في هذا القسم استدعاء البرامج النصية التكوين بأسماء محددة، مثل: **old-prerm** أو **new-postinst**. وهي، على التوالي، البرنامج النصي **prerm** الموجود في الإصدار القديم من الحزمة (مثبت قبل التحديث) والبرنامج النصي **postinst** الوارد في الإصدار الجديد (مثبت بواسطة التحديث).

١.٢.٤.٨. التثبيت وترقية تسلسل البرنامج النصي

إليك ما يحدث أثناء التثبيت (أو التحديث):

١. للحصول على تحديث، يستدعي **dpkg** إصدار *new-version* **prerm upgrade**.

٢. بعد التحديث، يقوم **dpkg** بعد ذلك بتنفيذ النسخة القديمة الجديدة قبل الترقية؛ بالنسبة للتثبيت الأول، يتم تنفيذ التثبيت الجديد قبل التثبيت. قد يضيف الإصدار القديم في المعلمة الأخيرة إذا تم تثبيت الحزمة وإزالتها بالفعل (ولكن لم يتم تطهيرها، فقد تم الاحتفاظ بملفات التكوين).

٣. ثم يتم تفريغ ملفات الحزمة الجديدة. في حالة وجود ملف بالفعل، يتم استبداله، ولكن يتم عمل نسخة احتياطية وتخزينه مؤقتًا.

٤. للحصول على التحديث، ينفذ **dpkg** إصدارًا جديدًا من ترقية **postrm** القديمة.

٥. يقوم **dpkg** بتحديث جميع البيانات الداخلية (قائمة الملفات، البرامج النصية للتكوين، وما إلى ذلك) ويزيل النسخ الاحتياطية للملفات المستبدلة. هذه هي نقطة اللاعودة: لم يعد **dpkg** قادرًا على الوصول إلى جميع العناصر اللازمة للعودة إلى الحالة السابقة.

٦. سيقوم **dpkg** بتحديث ملفات التكوين، ويطلب منك تحديد ما إذا كان غير قادر على إدارة هذه المهمة تلقائيًا. تمت مناقشة تفاصيل هذا الإجراء في القسم ٣.٤.٨، "المجموع الاختباري والملفات".

٧. وأخيرًا، يقوم **dpkg** بتكوين الحزمة عن طريق تنفيذ **new-postinst configure** *last-version-configured*.

٢.٢.٤.٨. إزالة الحزم

إليك ما يحدث أثناء إزالة الحزمة.

١. **dpkg** تستدعي **prerm remove**.

٢. يزيل **dpkg** جميع ملفات الحزمة، باستثناء ملفات التكوين ومخطوطات التكوين.

٣. تنفذ **dpkg** *remove* **postrm**. تتم إزالة كافة البرامج النصية للتكوين ، باستثناء postrm. إذا لم تستخدم خيار التطهير ، تتوقف العملية هنا.

٤. لتنظيف الحزمة بالكامل (الأمر الصادر مع **dpkg --purge** أو **dpkg -P**)، يتم أيضًا حذف ملفات التكوين، بالإضافة إلى عدد معين من النسخ (***.dpkg-tmp, *.dpkg-old, *.dpkg-new**) والملفات المؤقتة؛ ثم ينفذ **dpkg** عملية التطهير بعد الوضع.

في بعض الحالات، قد تستخدم الحزمة **debconf** لطلب معلومات التكوين منك: ثم يتم استكمال النصوص الأربعة المفصلة أعلاه ببرنامج نصي للتكوين مصمم لاكتساب تلك المعلومات. أثناء التثبيت، يحدد هذا البرنامج النصي بالتفصيل الأسئلة التي سيطرحها **debconf**. يتم تسجيل الردود في قاعدة بيانات **debconf** للرجوع إليها في المستقبل. يتم تنفيذ البرنامج النصي بشكل عام قبل **apt** قبل تثبيت الحزم واحدًا تلو الآخر من أجل تجميع جميع الأسئلة معًا في بداية العملية. يمكن أن تستخدم البرامج النصية قبل التثبيت وبعده هذه المعلومات للعمل وفقًا لرغباتك.

أداة debconf

يتم إنشاء أداة **debconf** لحل مشكلة متكررة في دبيان. جميع حزم دبيان غير قادرة على العمل بدون حد أدنى من التكوين المستخدم لطرح الأسئلة مع المكالمات إلى الأوامر **echo** و**read** الأوامر في **postinst** البرامج النصية للصدفة (وغيرها من البرامج النصية المشابهة). وقد أجبر هذا المثبت على تثبيت عمليات التثبيت أو التحديثات الكبيرة من أجل الاستجابة لاستفسارات التكوين المختلفة عند ظهورها. لقد تم الاستغناء عن هذه التفاعلات اليدوية بالكامل تقريبًا، بفضل **debconf**.

تحتوي أداة **debconf** على العديد من الميزات المثيرة للاهتمام: فهي تتطلب من المطور تحديد تفاعل المستخدم؛ يسمح بترجمة جميع السلاسل المعروضة (يتم تخزين جميع الترجمات في ملف **templates** التي تصف التفاعلات)؛ يوفر واجهات مختلفة للأسئلة (وضع النص، الوضع الرسومي، غير تفاعلي)؛ ويسمح بإنشاء قاعدة بيانات مركزية للاستجابات لمشاركة نفس التكوين مع العديد من أجهزة الحاسوب. الميزة الأكثر أهمية هي أنه يمكن تقديم جميع الأسئلة في سطر واحد، دفعة واحدة، قبل بدء عملية تثبيت أو تحديث طويلة. الآن، يمكنك القيام بأعمالك بينما يقوم النظام بمعالجة التثبيت من تلقاء نفسه، دون الحاجة إلى البقاء هناك والنظر للشاشة، في انتظار ظهور الأسئلة.

٣.٤.٨. المجموع الاختباري، Conffiles

بالإضافة إلى برامج المشرف النصية وبيانات التحكم التي سبق ذكرها في الأقسام السابقة، قد يحتوي أرشيف **control.tar.gz** الخاص بحزمة ديبان على ملفات أخرى مثيرة للاهتمام:

```
# ar p /var/cache/apt/archives/bash_4.4-2_amd64.deb control.tar.gz | tar -tzf -
./
./conffiles
./control
./md5sums
./postinst
./postrm
./preinst
./prerm
```

يحتوي الأول -**md5sums**- على المجموع الاختباري MD5 لجميع ملفات الحزمة. ميزته الرئيسية هي أنه يسمح لـ **dpkg --verify** بالتحقق مما إذا تم تعديل هذه الملفات منذ تثبيتها. لاحظ أنه عند عدم وجود هذا الملف، سيقوم **dpkg** بإنشائه ديناميكياً في وقت التثبيت (وتخزينه في قاعدة بيانات **dpkg** تماماً مثل ملفات التحكم الأخرى).

تسرد ملفات **conffiles** ملفات الحزمة التي يجب معالجتها كملفات تكوين. يمكن تعديل ملفات التكوين من قبل المسؤول، وسيحاول **dpkg** الاحتفاظ بهذه التغييرات أثناء تحديث الحزمة.

في الواقع، في هذه الحالة، يتصرف **dpkg** بذكاء قدر الإمكان: إذا لم يتغير ملف التكوين القياسي بين النسختين، فلن يفعل شيئًا. ومع ذلك، إذا تغير الملف، فسيحاول تحديث هذا الملف. هناك حالتان ممكنتان: إما أن المسؤول لم يلمس ملف التكوين هذا، وفي هذه الحالة يقوم **dpkg** تلقائيا بتثبيت الإصدار الجديد؛ أو تم تعديل الملف، وفي هذه الحالة يسأل **dpkg** المسؤول عن الإصدار الذي يرغب في استخدامه (الإصدار القديم مع التعديلات، أو الإصدار الجديد المقدم مع الحزمة). للمساعدة في اتخاذ هذا القرار، يعرض **dpkg** عرض **diff** يظهر الفرق بين النسختين. إذا اخترت الاحتفاظ بالإصدار القديم، فسيتم تخزين الإصدار الجديد في نفس الموقع في ملف بلاحقة **dpkg-dist.**. إذا اخترت الإصدار الجديد، فسيتم الاحتفاظ بالإصدار القديم في ملف به لاحقة **dpkg-old.**. يتكون الإجراء الآخر المتاح من مقاطعة **dpkg** للحظة لتحرير الملف ومحاولة إعادة التعديلات ذات الصلة (التي تم تحديدها مسبقًا باستخدام **diff**).

يتعامل **dpkg** مع تحديثات ملف التكوين، ولكن أثناء القيام بذلك، يقاطع عمله بانتظام لطلب إدخال من المسؤول. قد يكون هذا مضيعة للوقت وغير مريح. لحسن الحظ، يمكنك توجيه **dpkg** للرد على هذه المطالبات تلقائيًا. يحتفظ الخيار **force-confold**-- بالنسخة القديمة من الملف، بينما يستخدم **force-confnew**-- الإصدار الجديد. يتم احترام هذه الاختيارات، حتى إذا لم يتم تغيير الملف بواسطة المسؤول، والذي نادراً ما يكون له التأثير المطلوب. إن إضافة خيار --**force-confdef** يخبر **dpkg** بأن يقرر بنفسه متى كان ذلك ممكنًا (بمعنى آخر، عندما لا يتم لمس ملف التكوين الأصلي)، ويستخدم فقط **force-confnew**-- أو **force-confold**-- للحالات الأخرى.

تنطبق هذه الخيارات على **dpkg**، ولكن في معظم الأحيان سيعمل المسؤول مباشرة بـ **aptitude** أو **apt**. وبالتالي، من الضروري معرفة بناء الجملة المستخدم للإشارة إلى خيارات التمرير إلى الأمر **dpkg** (واجهات سطر الأوامر الخاصة بهم متشابهة جدًا).

```
$ apt -o DPkg::options::="--force-confdef" -o
DPkg::options::="--force-confold" full-upgrade
```

يمكن تخزين هذه الخيارات مباشرة في تكوين **apt**. للقيام بذلك، ما عليك سوى كتابة السطر التالي في الملف **/etc/apt/apt.conf.d/local**:

DPkg::options { "--force-confdef"; "--force-confold"; }

تضمين هذا الخيار في ملف التكوين يعني أنه سيتم استخدامه أيضًا في واجهة رسومية مثل **aptitude**.

وبالعكس، يمكنك أيضًا إجبار **dpkg** على طرح أسئلة ملف التكوين. يرشد خيار **--force-confask** لعرض الأسئلة حول ملفات التكوين، حتى في الحالات التي لا تكون فيها ضرورية عادةً. وبالتالي، عند إعادة تثبيت حزمة باستخدام هذا الخيار، سيطرح **dpkg** الأسئلة مرة أخرى لجميع ملفات التكوين التي قام المسؤول بتعديلها. هذا أمر مريح للغاية، خاصةً لإعادة تثبيت ملف التكوين الأصلي إذا تم حذفه ولم تكن هناك نسخة أخرى متاحة: لن تعمل إعادة التثبيت العادية، لأن **dpkg** يعتبر الإزالة شكلاً من أشكال التعديل الشرعي، وبالتالي لا يثبت ملف التكوين المطلوب.

٥.٨. ملخص

في هذا القسم، تعلمنا المزيد عن نظام حزم دبيان، وناقشنا أداة الحزمة المتقدمة " Advanced **P**ackage **T**ool" (APT) و **dpkg**، وتعلمنا عن تفاعل الحزمة الأساسية، وتكوين APT المتقدم والاستخدام، وتعمقنا في نظام حزم دبيان مع مرجع موجز عن تنسيق ملف **deb.**. نظرنا في ملف التحكم، وبرامج التهيئة النصية، والمجموع الاختباري، وملف **conffiles**.

نصائح ملخصة:

حزمة دبيان عبارة عن أرشيف مضغوط لتطبيق برمجي. يحتوي على ملفات التطبيق بالإضافة إلى البيانات الوصفية الأخرى بما في ذلك أسماء التبعيات التي يحتاجها التطبيق بالإضافة إلى النصوص البرمجية التي تمكن من تنفيذ الأوامر في مراحل مختلفة من دورة حياة الحزمة (التثبيت والإزالة والترقيات).

لا تحتوي أداة **dpkg**، بخلاف **apt** و **apt-get** (من عائلة APT)، على معرفة بجميع الحزم المتاحة التي يمكن استخدامها لتحقيق تبعيات الحزمة. وبالتالي، لإدارة حزم دبيان، من المرجح أن تستخدم الأدوات الأخيرة لأنها قادرة على حل مشكلات التبعية تلقائيًا.

يمكنك استخدام APT لتثبيت التطبيقات وإزالتها وتحديث الحزم وحتى ترقية نظامك بالكامل. فيما يلي النقاط الأساسية التي يجب أن تعرفها عن APT وتكوينها:

ملف **sources.list** هو ملف التكوين الرئيسي لتحديد مصادر الحزمة (أو المستودعات التي تحتوي على حزم).

تستخدم دبيان وكالي ثلاثة أقسام للتمييز بين الحزم وفقًا للتراخيص التي اختارها مؤلفو كل عمل: يحتوي **main** على جميع الحزم التي تتوافق تمامًا مع إرشادات دبيان للبرمجيات الحرة، يحتوي البرنامج **non-free** على برامج لا تتوافق (بالكامل) مع إرشادات البرمجيات الحرة ولكن مع ذلك يمكن توزيعها دون قيود، و **contrib** (المساهمات) تتضمن برمجيات مفتوحة المصدر لا يمكن أن تعمل بدون بعض العناصر غير الحرة.

تحتفظ Kali بالعديد من المستودعات بما في ذلك: **kali-rolling**، وهو المستودع الرئيسي للمستخدمين النهائيين ويجب أن يحتوي دائمًا على حزم قابلة للتثبيت وحديثة، **kali-dev**، الذي يستخدمه مطورو Kali وليس للاستخدام العام، و **kali-bleeding-edge**، والتي غالبًا ما تحتوي على حزم غير مجربة وغير مفحوصة يتم بناؤها تلقائيًا من مستودع Git (أو Subversion) الرئيسي بعد أقل من أربع وعشرين ساعة من انشائها.

عند العمل مع APT، يجب عليك أولاً تنزيل قائمة الحزم المتوفرة حاليًا مع التحديث المناسب.

يمكنك إضافة حزمة إلى النظام مع حزمة تثبيت بسيطة. ستقوم APT تلقائيًا بتثبيت التبعيات اللازمة.

لإزالة حزمة استخدم **apt remove** *package*. سيؤدي ذلك أيضًا إلى إزالة التبعيات العكسية للحزمة (أي الحزم التي تعتمد على الحزمة المراد إزالتها).

لإزالة جميع البيانات المرتبطة بالحزمة، يمكنك "تطهير" الحزمة باستخدام أمر **apt purge** *package*. على عكس الإزالة، لن يؤدي هذا إلى إزالة الحزمة فحسب، بل سيزيل أيضًا ملفات التكوين وأحيانًا بيانات المستخدم المرتبطة بها.

نوصي بإجراء ترقيات منتظمة لتثبيت آخر تحديثات الأمان. للترقية، استخدم **apt update** متبوعًا إما بترقية **apt upgrade** أو **apt-get upgrade** أو **aptitude safe-upgrade**. تبحث هذه الأوامر عن الحزم المثبتة التي يمكن ترقيتها دون إزالة أي حزم.

للحصول على ترقيات أكثر أهمية، مثل ترقيات الإصدار الرئيسية، استخدم **apt full-upgrade**. باستخدام هذا التعليمات، سيكمل **apt** الترقية حتى إذا كان عليه إزالة بعض الحزم القديمة أو تثبيت تبعيات جديدة. هذا هو الأمر الذي يجب عليك استخدامه للترقيات العادية لنظام Kali Rolling الخاص بك. راجع إيجابيات وسلبيات التحديثات التي أوضحناها في هذا الفصل.

يمكن استخدام العديد من الأدوات لفحص حزم ديبان:

يسرد *package* **dpkg --listfiles** (أو **L-**) الملفات التي تم تثبيتها بواسطة الحزمة المحددة.

يبحث *file* **dpkg --search** (أو **S-**) عن أي حزم تحتوي على الملف أو المسار الذي تم تمريره في الوسيطة.

يعرض **dpkg --list** (أو **l-**) قائمة الحزم المعروفة للنظام وحالة تثبيتها.

يسرد *file.deb* **dpkg --contents** (أو c-) جميع الملفات في ملف **deb.** معين.

يعرض *file.deb* **dpkg --info** (أو I-) رؤوس ملف **deb.** المحدد.

تعرض مختلف أوامر **apt-cache** الفرعية الكثير من المعلومات المخزنة في قاعدة بيانات APT الداخلية.

لتجنب الاستخدام المفرط للقرص، يجب أن تفرز بانتظام من خلال **/var/cache/apt/archives/**. يمكن استخدام أمرين لهذا: **apt clean** (أو **-apt**

get clean) يفرغ المجلد بالكامل. **apt autoclean (apt-get autoclean)** بإزالة الحزم التي لم يعد من الممكن تنزيلها لأنها اختفت من المرآة وبالتالي فهي عديمة الفائدة.

Aptitude هو برنامج تفاعلي يمكن استخدامه في الوضع شبه الرسومي على وحدة التحكم. إنه برنامج قوي للغاية يمكنه مساعدتك في تثبيت الحزم وإصلاحها.

synaptic هو مدير حزم رسومية يتميز بواجهة رسومية واضحة وفعالة.

كمستخدم متقدم، يمكنك إنشاء ملفات في **/etc/apt/apt.conf.d/** لتكوين جوانب معينة من APT. يمكنك أيضًا إدارة أولويات الحزم، وتتبع الحزم المثبتة تلقائيًا، والعمل مع العديد من التوزيع أو الهياكل في وقت واحد، استخدم توقيعات التشفير للتحقق من صحة الحزم، وترقية الملفات باستخدام التقنيات الموضحة في هذا الفصل.

على الرغم من أفضل جهود مشرفي Kali/Debian، فإن ترقية النظام ليست دائمًا سهلة كما نأمل. عندما يحدث ذلك، يمكنك إلقاء نظرة على أداة تعقب أخطاء Kali ونظام تتبع أخطاء دبيان على **https://bugs.debian.org/package** للتحقق مما إذا كانت المشكلة قد تم الإبلاغ عنها بالفعل. يمكنك أيضًا محاولة الرجوع إلى إصدار أقدم من الحزمة أو تصحيح البرنامج النصي لصاحب الحزمة العاطلة وإصلاحها.

التمرين الأول للفصل الثامن - إعادة توجيه المرآة

١. اكتشف أي مرآة ستلبي طلب تنزيل ISO الخاص بك، إذا كنت ستحاول تنزيل Kali ISO من cdimage.kali.org.

٢. تكوين إدخال مصدر في ملف **sources.list** الخاص بك. تحديث ذاكرة التخزين المؤقت للحزمة.

٣. أضف مستودع **kali-bleeding-edge** إلى نظامك وقم بتثبيت النسخة من الحزمة "`set`".

الإجابة:

١. تحقق من المرآة بـ:

```
curl -sI http://cdimage.kali.org/README
```

٢. لتمكين مستودعات المصدر، قم بإلغاء تعليق هذا السطر في **/etc/apt/sources.list**:

```
deb-src http://http.kali.org/kali kali-rolling
main contrib non-free
```

٣. لتمكين إعادة وضع **kali-bleeding-edge**، أضف هذا السطر إلى **/etc/apt/sources.list**:

```
deb http://http.kali.org/kali kali-bleeding-edge
contrib non-free main
```

بعد ذلك، قم بالمزامنة مع تحديث باستخدام **apt-get update**:

```
apt-get update
```

ثم قم بتثبيت إصدار bleeding edge من المجموعة "of set":

```
apt install set/kali-bleeding-edge
```

التمرين الثاني، للفصل الثامن - التعرف على dpkg.

١. أوجد المسار إلى لثنائيات **atk6-alive6**.
٢. حدد الحزمة التي قامت بتثبيتها والملفات الأخرى المضمنة في الحزمة.
٣. ابحث عن الحزم المثبتة محلياً والتي تحمل اسم "wifi".
٤. ابحث عن أدوات في مستودع كالي تحمل "wifi" باسمها.
٥. قائمة الملفات المثبتة التي نشأت من حزمة **nmap**.

الإجابة:

١. ابحث عن المسار:

```
which atk6-alive6
```

٢. حدد ما هو atk-alive6 المثبت والملفات الأخرى التي تتضمنها الحزمة:

```
dpkg -S atk6-alive6
```

٣. +٤. ابحث عن الحزم المثبتة محلياً والتي تحمل اسم "wifi".

```
dpkg -l |grep wifi
apt-cache search wifi |grep wifi
```

٥. ضع قائمة بالملفات التي نشأت من حزمة **nmap**:

```
dpkg -L nmap
```

التمرين الثالث، الفصل الثامن - اللعب باستخدام dpkg-deb

في هذا التمرين، نريد تثبيت Nessus. Nessus ليس مجرد تثبيت مناسب. بل إنها عملية:

- ❖ تنزيل ملف **deb.** من Nessus
- ❖ قم بتثبيت **deb.** بـ **dpkg**
- ❖ سجل Nessus واحصل على رمز التفعيل عبر البريد الإلكتروني
- ❖ إنشاء رمز التحدي "Generate a challenge code" لـ nessuscli في kali
- ❖ أرسل التحدي والتفعيل للوصول إلى الإضافات
- ❖ تنزيل الإضافات وتثبيتها

هذه عملية طويلة وليست بسيطة. باستخدام المهارات التي أظهرناها في هذا الفصل، قم بتنزيل Nessus وتثبيته وإنشاء حزمة تتضمن المكونات الإضافية وتثبيتها تلقائيًا.

- ❖ ابحث عن حزمة Nessus Debian المجانية وقم بتنزيلها وتثبيتها وتسجيلها.
- ❖ بدلاً من تثبيت المكوِّنات الإضافية برمجيًا من خلال واجهة الويب Nessus، احفظ الإضافات في ملف محلي.
- ❖ قم بتجميع توقيعات Nessus في حزمة **deb.** حتى تتمكن من تثبيت Nessus (لنقل عبر أجهزة حاسوب متعددة)، دون الحاجة إلى إعادة تحميل التوقيعات من كل حاسوب.
- ❖ قم بإنشاء حزمة **deb.** Nessus جديدة تقوم بتثبيت الإضافات تلقائيًا.

الإجابة:

أولاً، سيتعين عليك تثبيت Nessus بالطريقة "القياسية". هناك الكثير من الخطوات.

فديو لطريقة التثبيت في الصفحة:

https://kali.training/topic/exercise-8-3-playing-with-dpkg-deb/

١. استخراج الحزمة. هل تقوم بنسخ ولصق؟ لاحظ أن أرقام نسختك قد تختلف.

```
root@kali:~/Downloads# dpkg-deb -R Nessus-6.9.0-debian6_amd64.deb nessus #Raw extract the package
```

٢. سرد محتويات الحزمة:

```
ls -lR ./nessus
```

٤. انسخ ملف الإضافات إلى **/root/opt/nessus/var/nessus**:

```
cp /root/Downloads/all-2.0.tar.gz nessus/opt/nessus/var/nessus
```

قم بتحرير ملف ديبيان postinst، وابحث عن هذا القسم، وقم بإجراء التغييرات بالشكل المناسب:

```
nano nessus/DEBIAN/postinst
```

5. قم بتحرير ملف postinst لاستيراد التوقيعات دون اتصال. إضافة مكان ما في postinst:

```
echo "UBERHAX - Updating plugins from local file..."
rm -f ${NESSUS_PREFIX}/lib/nessus/plugins/MD5
${NESSUS_PREFIX}/sbin/nessuscli update ${NESSUS_PREFIX}/var/nessus/all-2.0.tar.gz
${NESSUS_PREFIX}/sbin/nessusd -R

test -f ${NESSUS_PREFIX}/etc/nessus/nessus-fetch.rc && {
	echo "Fetching the newest plugins from nessus.org..."
	rm -f ${NESSUS_PREFIX}/lib/nessus/plugins/MD5
	${NESSUS_PREFIX}/sbin/nessuscli update --plugins-only
	${NESSUS_PREFIX}/sbin/nessusd -R
}
```

دعونا نضع الثلج على الكعكة وننظف أنفسنا. احذف ملف التوقيع هذا لتوفير المساحة. سنفعل ذلك في ملف **postrm**:

```
rm -f ${NESSUS_PREFIX}/var/nessus/all-2.0.tar.gz
```

أعد حزم ملف **deb**. قد تختلف نسختك:

```
dpkg-deb -b nessus nessus_6.9.0_amd64.deb
```

التمرين الرابع، للفصل الثامن - كالي MultiArch

سيكون هذا تمرينًا ممتعًا لأنه بسيط إلى حد ما، ويستخدم بعض أوامر الحزمة التي تعلمتها ويسمح لك بتشغيل برامج Windows من داخل Kali، بفضل **Wine**. ومع ذلك، قد يبدو الأمر أكثر تعقيدًا بكثير مما هو عليه لأنه سيكون عليك تثبيت بنية أجنبية (i386).

١. أضف خيار بنية 32 bit لمثيل كالي الخاص بك باستخدام **dpkg**.
٢. تثبيت wine32
٣. قم بتشغيل برنامج الوندوز ipscan باستخدام Wine.

غذاء الفكر:

apt-cache search nmap ... لماذا الأداة "**atac**" في النتائج؟

الإجابات:

الحل مباشر إلى حد ما. ومع ذلك، لا تفوت الأمر i386. هذه هي نقطة التحول في التمرين، حيث نعمل في

```
root@kali:~# wine
it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first.  as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32"
Usage: wine PROGRAM [ARGUMENTS...]   Run the specified program
       wine --help                   Display this help and exit
       wine --version                Output version information and exit
root@kali:~# dpkg --print-architecture
root@kali:~# dpkg --add-architecture i386
root@kali:~# dpkg --print-foreign-architectures
root@kali:~# i386 # change architecture in new program environment
# apt update
# apt install wine32
# wget https://sourceforge.net/projects/ipscan/files/ipscan2-binary/2.21/ipscan221.exe/download -O ipscan221.exe
# wine ipscan221.exe
```

root : asciinema — Konsole

File Edit View Bookmarks Settings Help

```
HTTP request sent, awaiting response... 200 OK
Length: 111104 (108K) [application/octet-stream]
Saving to: 'ipscan221.exe'

ipscan221.exe          100%[==========================>] 108.50K   342KB/s    in 0.3s

2017-08-28 15:46:53 (342 KB/s) - 'ipscan221.exe' saved [111104/111104]

# wine ipscan221.exe
wine: created the configuration directory '/root/.wine'
err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-
c000-000000000046}
err:ole:marshal_object couldn                                    140c1-7436-11ce-
8034-00aa006009fa}
err:ole:StdMarshalImpl_Marsha                                    80004002
err:ole:CoMarshalInterface Fa                                    5-11ce-8034-00aa
006009fa}, 80004002
err:ole:get_local_server_stre
err:ole:marshal_object couldn                                    00131-0000-0000-
c000-000000000046}
err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-
8034-00aa006009fa}
err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa
006009fa}, 80004002
err:ole:get_local_server_stream Failed: 80004002
Could not load wine-gecko. HTML rendering will be disabled.
```

Wine

The Wine configuration in /root/.wine is being updated, please wait...

root : asciinema   root : bash

root : asciinema — Konsole

File Edit View Bookmarks Settings Help

```
Location: https://cytranet.dl.sourceforge.net/project/ipscan/ipscan2-binary/2.21/ipscan2
21.exe [following]
--2017-08-28 12:50:01--  https://cytranet.dl.sourceforge.net/project/ipscan/ipscan2-bina
ry/2.21/ipscan221.exe
Resolving cytranet.dl.sourceforge.net (cytranet.dl.sourceforge.net)... 74.82.59.181, 74.
82.59.181
Connecting to cytranet.dl.sourceforge.net (cytranet.dl.sourceforge.net)|74.82.59.181|:44
3... connected.
HTTP request sent, awaiting response... 200 OK
Length: 111104 (108K) [application/octet-stream]
Saving to: 'ipscan221.exe'

ipscan221.exe          100%[=======

2017-08-28 12:50:02 (731 KB/s) - '

root@kali:~# wine ipscan221.exe
```

root : asciinema

Angry IP Scanner 2.21

File Go to Commands Favorites Options Utils Help

IP range: . . . to . . . Start

Hostname: kali IP Threads 0

IP | Ping | Hostname

The list is empty. Set the IP range and click Start to start scanning.

Ready

اختبار الشهادة للفصل الثامن

١. ما الأداة التي تقوم بتثبيت الحزم مباشرةً دون النظر إلى التبعيات أو الحزم الأخرى؟

- o apt-get
- o dpkg
- o aptitude
- o apt

٢. ما الأداة التي هي نظام إدارة حزم كامل مصمم لتثبيت التطبيقات وإزالتها وتحديث الحزم وحتى ترقية نظامك بالكامل؟

- o dpkg
- o Advanced Package Tool
- o Package Updater
- o /usr/bin/gnome-software

٣. ما هو ملف التكوين الرئيسي لتحديد مصادر الحزمة؟

- o /etc/apt/sources.list.d/list
- o /etc/sources
- o /etc/sources.list
- o /etc/apt/sources.list

٤. اختر وصف مصدر apt الصحيح بشكل صحيح:

- deb http://http.kali.org/kali kali main non-free contrib
- deb ssh://http.kali.org/kali kali-rolling main non-free contrib
- deb http://http.kali.org/kali kali-rolling main free contrib
- deb http://http.kali.org/kali kali-rolling main non-free contrib

٥. أي وصف مصدر مناسب يشير إلى برنامج لا يتوافق مع إرشادات ديبان للبرمجيات الحرة؟

- deb http://http.kali.org/kali kali-rolling main free contrib
- deb http://http.kali.org/kali kali-rolling main contrib
- deb http://http.kali.org/kali kali-rolling main non-free contrib
- deb http://http.kali.org/kali kali-rolling main extras contrib

٦. أي من المستودعات التالية موصى بها لمعظم المستخدمين؟

- kali bleeding-edge
- kali-linux-full
- kali-rolling
- kali-dev
- kali-linux

٧. أي أمر يقوم بتثبيت حزمة man-db؟

o dpkg man-db_2.7.0.2-5_amd64.deb

o dpkg -I man-db_2.7.0.2-5_amd64.deb

o dpkg -install man-db_2.7.0.2-5_amd64.deb

o dpkg -i man-db_2.7.0.2-5_amd64.deb

٨. ما هو الأمر الذي يجب استخدامه للتحديثات المنتظمة لـ Kali Linux وسيزيل الحزم القديمة وتثبيت التبعيات الجديدة؟

o apt-get full-update

o apt-get full-upgrade

o apt-get update

o apt-get upgrade

٩. أي من الأوامر التالية يقوم بتنزيل أحدث قائمة من الحزم المتاحة، ويجب تشغيله قبل تشغيل **apt**؟

o apt-get update

o apt update

o apt-update

١٠. أي من أمر سيعرض كل ملفات حزمة metaploit-framework؟

o aptitude search metasploit-framework

o dpkg -L metasploit-framework

o apt list metasploit-framework

o apt-search metasploit-framework

١١. أي من الأوامر التالية سيعرض اسم الحزمة التي قامت بتنزيل "msfconsole"؟

- o dpkg -S msfconsole
- o apt list msfconsole
- o aptitude search msfconsole
- o apt-search msfconsole

١٢. أي من الأوامر التالية سيعرض كل الحزم الموجودة في النظام؟

- o dpkg -l
- o apt list
- o apt search
- o apt-search

١٣. عندما تريد تثبيت حزمة للمعالج أخر غير الموجود في حاسوبك. كيف ستمكن هذا؟

- o apt-get install kali-linux-foreign
- o apt -a
- o dpkg –add-architecture
- o apt config –enable-foreign-architecture

١٤. أي مما يلي يدير الحزم بالواجهة الرسومية؟

- o aptitude
- o synaptic
- o dpkg
- o apt

١٥. أي من الأوامر التالية سيعرض البنية المثبتة للنظام الحالي؟

- apt print architectures
- arch –list
- dpkg –print-architecture
- aptitude list architectures

١٦. أي ملف يحتوي على أغلب المعلومات الحيوية عن حزم دبيبان؟

- .deb
- package-list
- .pkginfo
- control.tar.gz

١٧. أي مما يلي ليس جزءًا من حزمة دبيان القياسية؟

- debian-binary
- manifest
- data.tar.xz
- control.tar.gz

١٨. أي ملف في حزم دبيان يحتوي على الملفات الفعلية المراد تثبيتها على نظام الملفات؟

- debian-binary
- package.tar.gz
- manifest
- data.tar.xz

١٩.	أي حقل في رأس الحزمة سيتسبب في رفض dpkg تثبيت حزمة وتشغيل apt لحل المشكلة عن طريق تحديث الحزمة غير المتوافقة إلى إصدار أحدث؟

- Updates
- Conflicts
- Breaks
- Incompat

٢٠.	أي مما يلي ليس نصًا برمجيًا صالحاً لتهيئة حزمة دبيان؟

- postinst
- preinst
- postconf
- postrm

الأجابات:

1. dpkg
2. Advanced Package Tool
3. /etc/apt/sources.list
4. deb http://http.kali.org/kali kali-rolling main non-free contrib
5. deb http://http.kali.org/kali kali-rolling main non-free contrib
6. kali-rolling
7. dpkg -i man-db_2.7.0.2-5_amd64.deb
8. apt-get full-upgrade
9. apt update
10. dpkg -L metasploit-framework
11. dpkg -S msfconsole
12. dpkg -l
13. dpkg –add-architecture
14. aptitude, synaptic
15. dpkg –print-architecture
16. control.tar.gz
17. manifest
18. data.tar.xz
19. Breaks
20. postconf

---((الفصل التاسع))---

9. الإستخدام المتقدم

تم بناء Kali كإطار اختبار الاختراق ذو وحدات عالية وقابل للتخصيص ويسمح ببعض التخصيص والاستخدام المتقدم إلى حد ما. يمكن أن تحدث التخصيصات على مستويات متعددة، بدءًا من مستوى التعليمات البرمجية المصدر. مصادر جميع حزم كالي متاحة للجمهور. في هذا الفصل، سنوضح كيف يمكنك استرداد الحزم وتعديلها وبناء الحزم المخصصة الخاصة بك خارجها. نواة لينكس هي حالة خاصة نوعًا ما، وعلى هذا النحو، يتم تغطيتها في قسم مخصص (القسم ٩.٢، "إعادة تجميع نواة لينكس")، حيث سنناقش مكان العثور على المصادر، وكيفية تكوين بنية النواة، وأخيرًا كيفية تجميعها وكيفية بناء حزم النواة المرتبطة بها.

المستوى الثاني من التخصيص هو في عملية بناء صور ISO حية. سنعرض كيف تقدم أداة الإنشاء المباشر الكثير من الخطافات وخيارات التكوين لتخصيص صورة ISO الناتجة، بما في ذلك إمكانية استخدام حزم دبيان المخصصة بدلاً من الحزم المتوفرة على المرايا.

سنناقش أيضًا كيف يمكنك إنشاء ISO مباشر مستمر مدمج على مفتاح USB يحافظ على الملفات وتغييرات نظام التشغيل بين عمليات إعادة التشغيل.

١.٩. تعديل حزم kali

عادة ما يكون تعديل حزم Kali مهمة للمساهمين والمطورين في Kali: يقومون بتحديث الحزم بإصدارات جديدة من المنبع، أو تعديل التكوين الافتراضي من أجل تكامل أفضل في التوزيع، أو إصلاح الأخطاء التي أبلغ عنها المستخدمون. ولكن قد يكون لديك احتياجات محددة لم يتم تلبيتها من خلال الحزم الرسمية ومعرفة كيفية بناء حزمة معدلة يمكن أن تكون ذات قيمة كبيرة.

قد تتساءل لماذا تحتاج إلى عناء مع الحزمة على الإطلاق. بعد كل شيء، إذا كان عليك تعديل جزء من البرنامج، فيمكنك دائمًا الحصول على شفرة المصدر الخاصة به (عادةً باستخدام **git**) وتشغيل النسخة المعدلة مباشرة من مصدر خارجي. لا بأس بهذا عندما يكون ذلك ممكنًا وعندما تستخدم مجلد home الخاص بك لهذا الغرض، ولكن إذا كان تطبيقك يتطلب إعدادًا على مستوى النظام (على سبيل المثال، مع خطوة التثبيت "**make install**")، فسيؤدي ذلك إلى تلويث نظام الملفات الخاص بك بالملفات غير المعروفة لـ **dpkg** وسوف يخلق قريباً مشاكل لا يمكن اكتشافها من خلال تبعيات الحزمة. علاوة على ذلك، مع الحزم المناسبة، ستتمكن من مشاركة تغييراتك ونشرها على أجهزة حاسوب متعددة بسهولة أكبر أو إرجاع التغييرات بعد اكتشاف أنها لم تكن تعمل كما كنت تأمل.

إذن متى تريد تعديل الحزمة؟ دعنا نلقي نظرة على بعض الأمثلة. أولاً، سنفترض أنك مستخدم كثيف لـ SET ولاحظت إصدارًا جديدًا من المصدر ولكن مطوري Kali مشغولون جميعًا بعقد مؤتمر وتريد تجربته على الفور. تريد تحديث الحزمة بنفسك. في حالة أخرى، سنفترض أنك تكافح من أجل تشغيل بطاقة MIFARE NFC الخاصة بك وتريد إعادة بناء "libfreefare" لتمكين

رسائل التصحيح من أجل الحصول على بيانات قابلة للتنفيذ لتقديمها في تقرير الخطأ الذي تقوم بإعداده حاليًا. في الحالة الأخيرة، سنفترض أن برنامج "pyrit" فشل مع ظهور رسالة خطأ مشفرة. بعد البحث على الويب، تجد التزامًا نتوقع إصلاح مشكلتك في مستودع GitHub الرئيسي وترغب في إعادة إنشاء الحزمة مع تطبيق هذا الإصلاح.

سنتناول جميع هذه العينات في الأقسام التالية. سنحاول تعميم التفسيرات بحيث يمكنك تطبيق التعليمات بشكل أفضل على الحالات الأخرى ولكن من المستحيل تغطية جميع المواقف التي قد تواجهها. إذا واجهت مشاكل، فقم بتطبيق أفضل حكم لك للعثور على حل أو انتقل لطلب المساعدة في المنتديات الأكثر ملاءمة (انظر الفصل السادس، الحصول على المساعدة).

مهما كان التغيير الذي تريد إجراؤه، فإن العملية العامة دائمًا ما تكون هي نفسها: احصل على الحزمة المصدر، واستخرجها، وأدخل التغييرات، ثم أنشئ الحزمة. ولكن لكل خطوة، غالبًا ما تكون هناك أدوات متعددة يمكنها التعامل مع المهمة. لقد اخترنا الأدوات الأكثر صلة والأكثر شيوعًا، لكن مراجعتنا ليست شاملة.

٩.١.١. الحصول على المصادر

تبدأ إعادة بناء حزمة كالي بالحصول على الكود المصدر الخاصة بها. تتكون حزمة المصدر من ملفات متعددة: الملف الرئيسي هو ملف **dsc.*** (التحكم في مصدر دبيان) حيث يسرد الملفات المصاحبة الأخرى، والتي يمكن أن تكون **tar.***{gz,bz2,xz}*.*، وأحيانًا **diff.gz.*** أو ملفات **debian.tar.***{gz,bz2,xz}*.*.

يتم تخزين الحزم المصدر على مرايا كالي المتوفرة عبر HTTP. يمكنك استخدام متصفح الويب الخاص بك لتنزيل جميع الملفات المطلوبة ولكن أسهل طريقة لتحقيق ذلك هي استخدام الأمر: `apt source` *source_package_name*. يتطلب هذا الأمر سطر **deb-src** في ملف **/etc/apt/sources.list/** وملفات الفهرس المحدثة (التي يتم تنفيذها بتشغيل **apt update**). بشكل افتراضي، لا يضيف Kali السطر المطلوب حيث يحتاج عدد قليل من مستخدمي Kali فعلياً إلى استرداد حزم المصدر ولكن يمكنك إضافته بسهولة (راجع نموذج الملف في القسم ٣.١.٨، "مستودعات Kali" والتفسيرات المرتبطة في القسم ٢.١.٨، "فهم ملف sources.list").

```
$ apt source libfreefare
[...]
$ cd libfreefare-0.4.0
$ ls
AUTHORS    CMakeLists.txt  COPYING   HACKING         m4           README
ChangeLog  configure.ac    debian    libfreefare     Makefile.am  test
cmake      contrib         examples  libfreefare.pc.in  NEWS      TODO
$ ls debian
changelog  copyright               libfreefare-dev.install  rules
compat     libfreefare0.install    libfreefare-doc.install  source
control    libfreefare-bin.install README.Source            watch
```

في هذا المثال، بينما تلقينا الحزمة المصدر من مرآة كالي، فإن الحزمة هي نفسها كما في ديبيان نظراً لأن سلسلة الإصدار لا تحتوي على "kali". هذا يعني أنه لم يتم تطبيق أي تغييرات خاصة بالكالي.

إذا كنت بحاجة إلى إصدار محدد من حزمة المصدر، والذي لا يتوفر حاليًا في المستودعات المدرجة في **/etc/apt/sources.list**، فإن أسهل طريقة لتنزيلها هي معرفة عنوان URL للملف **.dsc** الخاص بها عن طريق البحث على http://pkg.kali.org ثم تسليم عنوان URL هذا إلى **dget** (من حزمة devscripts).

بعد البحث عن عنوان URL لحزمة مصدر libreefare المتوفرة في kali-bleeding-edge، يمكنك تنزيله باستخدام **dget**. سيقوم أولاً بتنزيل ملف **.dsc**، ثم تحليله لمعرفة الملفات الأخرى المشار لها، ثم تنزيلها من نفس الموقع:

```
$ dget http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc
dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   364  100   364    0     0    852      0 --:--:-- --:--:-- --:--:--   854
100  1935  100  1935    0     0   2650      0 --:--:-- --:--:-- --:--:-- 19948
dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git1439352548.ffde4d.orig.tar.gz
[...]
```

dget: retrieving http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~git1439352548.ffde4d-1.debian.tar.xz

[...]

libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc:

dscverify: libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc failed signature check:

gpg: Signature made Wed Aug 12 06:14:03 2015 CEST

gpg: using RSA key 43EF73F4BD8096DA

gpg: Can't check signature: No public key

Validation FAILED!!

$ dpkg-source -x `libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc`

gpgv: Signature made Wed Aug 12 06:14:03 2015 CEST

gpgv: using RSA key 43EF73F4BD8096DA

gpgv: Can't check signature: No public key

dpkg-source: warning: failed to verify signature on ./libfreefare_0.4.0+0~git1439352548.ffde4d-1.dsc

dpkg-source: info: extracting libfreefare in libfreefare-0.4.0+0~git1439352548.ffde4d

dpkg-source: info: unpacking libfreefare_0.4.0+0~git1439352548.ffde4d.orig.tar.gz

dpkg-source: info: unpacking libfreefare_0.4.0+0~git1439352548.ffde4d-1.debian.tar.xz

تجدر الإشارة إلى أن **dget** لم تستخرج الحزمة المصدر تلقائيًا لأنها لم تستطع التحقق من توقيع PGP على الحزمة المصدر. وهكذا قمنا بهذه الخطوة يدويًا باستخدام ملف **dpkg-source -x** *dsc-file*. يمكنك أيضًا فرض استخراج الحزمة المصدر بتمرير الخيار **--allow-unauthenticated** أو خيار **-u**.

وبالعكس، يمكنك استخدام **--download-only** لتخطي خطوة استخراج الحزمة المصدر.

استرجاع المصادر من Git

ربما لاحظت أن استدعاء المصدر المناسب يخبرك عن مستودع Git محتمل يستخدم للحفاظ على الحزمة. قد يشير إلى مستودع دبيان جيت أو مستودع كالي جيت.

يتم الاحتفاظ بجميع الحزم الخاصة بـ Kali في مستودعات Git المستضافة على gitlab.com/kalilinux. يمكنك استرداد المصادر من تلك المستودعات باستخدام:

```
git clone https://gitlab.com/kalilinux/packages/source-package.git
```

على عكس ما تحصل عليه باستخدام **apt source**، لن يتم تطبيق التصحيحات تلقائيًا على الشجرة التي تم الحصول عليها. ألق نظرة على **debian/patches/** لمعرفة المزيد عن التغييرات المحتملة التي قام بها Kali.

```
$ git clone https://gitlab.com/kalilinux/packages/kali-meta.git
Cloning into 'kali-meta'...
remote: Counting objects: 760, done.
remote: Compressing objects: 100% (614/614), done.
```

```
remote: Total 760 (delta 279), reused 0 (delta 0)
Receiving objects: 100% (760/760), 141.01 KiB | 0 bytes/s, done.
Resolving deltas: 100% (279/279), done.
Checking connectivity... done.
```

```
$ cd kali-meta
$ ls
debian
$ ls debian
changelog  compat  control  copyright  rules  source
```

يمكنك استخدام مستودعات git كطريقة أخرى لاسترداد المصادر، وبالتالي (في الغالب) اتبع الإرشادات الأخرى من هذا القسم. ولكن عندما يعمل مطورو Kali مع هذه المستودعات، يستخدمون سير عمل تغليف آخر ويستخدمون أدوات من حزمة git-buildpackage التي لن نغطيها هنا. يمكنك معرفة المزيد عن هذه الأدوات هنا: https://honk.sigxcpu.org/piki/projects/git-buildpackage/

٢.١.٩. تثبيت تبعيات البناء

الآن بعد أن حصلت على المصادر، ما زلت بحاجة إلى تثبيت تبعيات البناء. ستكون ضرورية لبناء الحزم الثنائية المرغوبة ولكن من المحتمل أيضًا أنها مطلوبة للبنى الجزئية التي قد ترغب في تشغيلها لاختبار التغييرات أثناء إجرائها.

تعلن كل حزمة مصدر عن تبعيات البناء الخاصة بها في حقل **Build-Depends** في ملف **debian/control**. دعنا نوجه تعليمات **apt** لتثبيت ذلك (على افتراض أنك في مجلد يحتوي على حزمة مصدر غير معبأة):

```
$ sudo apt build-dep ./
Note, using directory './' to get the build dependencies
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  autoconf automake autopoint autotools-dev debhelper dh-autoreconf
  dh-strip-nondeterminism gettext intltool-debian libarchive-zip-perl
  libfile-stripnondeterminism-perl libtool po-debconf
0 upgraded, 13 newly installed, 0 to remove and 0 not upgraded.
Need to get 4 456 kB of archives.
After this operation, 14,6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
[…]
```

في هذه العينة، يمكن أن تكون جميع تبعيات البناء راضية عن الحزم المتاحة لـ APT. قد لا يكون هذا هو الحال دائمًا لأن بناء الأدوات kali-rolling لا يضمن قابلية تثبيت تبعيات البناء (يتم فقط أخذ تبعيات الحزم الثنائية في الاعتبار). من الناحية العملية، غالبًا ما يتم ربط التبعيات الثنائية وتبعيات البناء بإحكام، ومعظم الحزم ستجعل تبعيات البناء الخاصة بها مرضية.

٣.١.٩. إجراء التغييرات

لا يمكننا تغطية جميع التغييرات المحتملة التي قد ترغب في إجرائها على حزمة معينة في هذا القسم. هذا من شأنه أن يعلمك كل التفاصيل الدقيقة عن حزم دبيان. ومع ذلك، سنغطي حالات الاستخدام الشائعة الثلاثة التي تم عرضها سابقًا وسنشرح بعض الأجزاء التي لا يمكن تجنبها (مثل الاحتفاظ بملف سجل التغييرات "**changelog**").

أول شيء يجب فعله هو تغيير رقم إصدار الحزمة بحيث يمكن تمييز الحزم المعاد بناؤها عن الحزم الأصلية التي تقدمها Kali أو Debian. لتحقيق ذلك، نضيف عادة لاحقة تحدد الكيان (الشخص أو الشركة) الذي يطبق التغييرات. بما أن **buxy** هو لقب **IRC** الخاص بي، فسأستخدمه كلاحقة. يتم تنفيذ مثل هذا التغيير بشكل أفضل باستخدام الأمر **`dch`** (*Debian CHangelog*) من حزمة devscripts، باستخدام أمر مثل **`dch --local buxy`**. يستدعي هذا محرر نص (**sensible-editor**، يقوم بتشغيل المحرر المعين في متغيرات بيئة **VISUAL** أو **EDITOR**، أو **/usr/bin/editor** بخلاف ذلك)، مما يسمح لك بتوثيق الاختلافات التي قدمتها عملية إعادة البناء هذه. يظهر هذا المحرر أن **`dch`** قد غيرت بالفعل ملف **debian/changelog**:

```
$ head -n 1 debian/changelog
libfreefare (0.4.0-2) unstable; urgency=low
```

```
$ dch --local buxy
[...]
$ head debian/changelog
libfreefare (0.4.0-2buxy1) UNRELEASED; urgency=medium

  * Enable --with-debug configure option.

-- Raphael Hertzog<buxy@kali.org>  Fri, 22 Apr 2016 10:36:00 -0400

libfreefare (0.4.0-2) unstable; urgency=low

  *  Update debian/copyrtight.

     Fix license to LGPL3+.
```

إذا كنت تقوم بهذه التغييرات بانتظام، فقد ترغب في تعيين متغيري البيئة **DEBFULLNAME** و **DEBEMAIL** على اسمك الكامل وعنوان بريدك الإلكتروني، على التوالي. سيتم استخدام قيمها من قبل العديد من أدوات التعبئة والتغليف، بما في ذلك **dch**، والتي ستقوم بدمجها على سطر trailer الموضح أعلاه (المبدوء بـ "--").

٩.١.٣.١. تطبيق التصحيح

في إحدى حالات الاستخدام لدينا، قمنا بتنزيل حزمة مصدر pyrit ونريد تطبيق التصحيح الذي وجدناه في مستودع git upstream. هذه عملية شائعة ويجب أن تكون دائمًا بسيطة. لسوء الحظ، يمكن معالجة التصحيحات بطرق مختلفة اعتمادًا على تنسيق الحزمة المصدر وعلى سير عمل حزمة Git المستخدم (عند استخدام Git لصيانة الحزمة).

٩.١.٣.١.١. مع حزمة مصدر غير معبأة

لقد قمت بتشغيل **apt source pyrit** ولديك مجلد **pyrit-0.4.0**. يمكنك تطبيق التصحيح الخاص بك مباشرة باستخدام **patch -p1** < *patch-file*:

```
$ apt source pyrit
[...]
$ cd pyrit-0.4.0
$ wget
https://github.com/JPaulMora/Pyrit/commit/14ec9971
74b8e8fd20d22b6a97c57e19633f12a0.patch -O
/tmp/pyrit-patch
[...]
$ patch -p1
```

في هذه المرحلة، قمت بتصحيح كود المصدر يدويًا ويمكنك بالفعل إنشاء حزم ثنائية من نسختك المعدلة (انظر القسم ٩.١.٤، "بدء الإنشاء"). ولكن إذا حاولت إنشاء حزمة مصدر محدثة، فسوف تفشل، وتشكو من "تغييرات في المصدر غير متوقعة". هذا لأن **pyrit** (مثل غالبية حزم المصدر) يستخدم تنسيق المصدر (انظر ملف **debian/source/format**) المعروف باسم ٣.٠

(quilt)، حيث يجب تسجيل التغييرات في كود المصدر في تصحيحات منفصلة مخزنة في **/debian/patches** وحيث يشير ملف **debian/patches/series** إلى الترتيب الذي يجب تطبيق التصحيحات عليه. يمكنك تسجيل تغييراتك في رقعة جديدة عن طريق تشغيل **dpkg-source --commit**:

```
$ dpkg-source --commit
dpkg-source: info: local changes detected, the modified files are:
 pyrit-0.4.0/cpyrit/pckttools.py
Enter the desired patch name: fix-for-scapy-2.3.patch
dpkg-source: info: local changes have been recorded in a new patch:
pyrit-0.4.0/debian/patches/fix-for-scapy-2.3.patch
$ tail -n 1 debian/patches/series
fix-for-scapy-2.3.patch
```

سلسلة تصحيح patch

لقد تم تعميم اتفاقية إدارة التصحيح هذه بواسطة أداة تسمى **quilt**، وبالتالي فإن تنسيق حزمة المصدر "٣.٠ (quilt)" متوافق مع هذه الأداة - مع الانحراف الصغير الذي تستخدمه **debian/patches** بدلاً من التصحيحات. تتوفر هذه الأداة في حزمة تحمل نفس الاسم ويمكنك العثور على برنامج تعليمي جميل هنا:
https://raphaelhertzog.com/2012/08/08/how-to-use-quilt-to-manage-patches-in-debian-packages/

إذا كانت الحزمة المصدر تستخدم تنسيق المصدر ١.٠ أو ٣.٠ (الأصلي)، فليس هناك ما يلزم لتسجيل تغييرات الإرسال في التصحيح. يتم تجميعها تلقائياً في حزمة المصدر الناتجة.

٢.١.٣.١.٩. مع مستودع Git

إذا كنت قد استخدمت Git لاسترداد حزمة المصدر، فإن الوضع أكثر تعقيدًا. هناك العديد من مهام سير عمل Git والأدوات المرتبطة بها، ومن الواضح أن جميع حزم دبيان لا تستخدم نفس سير العمل والأدوات. لا يزال التمييز الموضح بالفعل حول تنسيق المصدر ملائمًا، ولكن يجب عليك أيضًا التحقق مما إذا كانت التصحيحات مطبقة مسبقًا في شجرة المصدر أو ما إذا كانت مخزنة فقط في **debian/patches** (في هذه الحالة، يتم تطبيقها بعد ذلك في وقت البناء).

الأداة الأكثر شعبية هي git-buildpackage. هذا ما نستخدمه لإدارة جميع المستودعات في gitlab.com/kalilinux/packages. عند استخدامه، لا يتم تطبيق التصحيحات مسبقًا في شجرة المصدر ولكن يتم تخزينها في debian/patches. يمكنك إضافة التصحيحات يدويًا في هذا المجلد وإدراجها في debian/patches/series ولكن يميل مستخدمو git-buildpackage إلى استخدام **gbp pq** لتحرير سلسلة التصحيح بالكامل كفرع واحد يمكنك تمديده أو إعادة تصميمه حسب رغبتك. تحقق من gbp-pq(1) لمعرفة كيفية استدعاؤه.

git-dpm (مع الأمر المرتبط بنفس الاسم) هو أداة تغليف **git** أخرى يمكنك العثور عليها قيد الاستخدام. يسجل البيانات الوصفية في **debian/.git-dpm** ويحتفظ بالتصحيحات المطبقة في شجرة المصدر عن طريق دمج فرع مُعاد إصلاحه باستمرار يُنشئه من محتوى **debian/patches**.

٢.٣.١.٩. تعديل خيارات البناء

عادةً ما يتعين عليك تعديل خيارات البناء عندما تريد تمكين ميزة أو سلوك اختياري لم يتم تنشيطه في الحزمة الرسمية، أو عندما تريد تخصيص المعلمات التي تم تعيينها في وقت البناء من خلال خيار **configure**/. أو من خلال المتغيرات المحددة في بيئة البناء.

في هذه الحالات، تقتصر التغييرات عادةً على **debian/rules**، التي تدفع الخطوات في عملية بناء الحزمة. في أبسط الحالات، من السهل تحديد الأسطر المتعلقة بالتهيئة الأولية (**configure**/. ...) أو البناء الفعلي (**... (MAKE)$** أو **... make**). إذا لم يتم استدعاء هذه الأوامر بشكل صريح، فربما تكون أحد الآثار الجانبية لأمر صريح آخر، وفي هذه الحالة، يرجى الرجوع إلى وثائقها لمعرفة المزيد حول كيفية تغيير السلوك الافتراضي. مع الحزم التي تستخدم **dh**، قد تحتاج إلى إضافة تجاوز للأوامر **dh_auto_configure** أو **dh_auto_build** (راجع صفحات الدليل الخاصة بها للحصول على توضيحات حول كيفية تحقيق ذلك).

لجعل هذه التفسيرات أكثر واقعية، دعنا نطبقها على نموذج حالة الاستخدام لدينا. لقد قررت تعديل libfreefare لتمرير خيار **enable-debug--** للبرنامج النصي **configure**/. حتى تتمكن من الحصول على إخراج مطول من أدوات الاتصال بالحقل القريب (NFC) وتقديم تقرير خطأ أفضل حول Mifare غير المعترف به بطاقة NFC. نظراً لأن الحزمة تستخدم **dh** لقيادة عملية البناء، فأنت تضيف (أو في هذه الحالة تعدل) الهدف **override_dh_auto_configure**. في ما يلي المقتطف المقابل من ملف **debian/rules** libfreefare:

```
override_dh_auto_configure:
        dh_auto_configure -- --without-cutter --disable-silent-rules --enable-debug
```

٣.٣.١.٩. تغليف نسخة جديدة من المصدر

دعونا نلقي نظرة على مثال في هذه المرحلة، حيث نناقش حزم الإصدارات الأولية. لنفترض أنك مستخدم محترف لـ SET ولاحظت إصدارًا جديدًا من المصدر (٥.٤.٧) لم يتوفر بعد في Kali (التي تحتوي على الإصدار ٤.٤.٧ فقط). تريد بناء حزمة محدثة وتجربتها. يعد هذا إصدارًا ثانويًا، وبالتالي لا نتوقع أن يتطلب التحديث أي تغيير على مستوى التعبئة.

لتحديث حزمة المصدر، يمكنك استخراج مصدر tar الجديد بجوار حزمة المصدر الحالية ونسخ مجلد دبيان من حزمة المصدر الحالية إلى الحزمة الجديدة. ثم تقوم بتحريك النسخة في **debian/changelog.**

```
$ apt source set
Reading package lists... Done
NOTICE: 'set' packaging is maintained in the 'Git' version control system at:
git://gitlab.com/kalilinux/packages/set.git
Please use:
git clone git://gitlab.com/kalilinux/packages/set.git
to retrieve the latest (possibly unreleased) updates to the package.
Need to get 42.3 MB of source archives.
[...]
dpkg-source: warning: failed to verify signature on ./set_7.4.4-0kali1.dsc
```

```
dpkg-source: info: extracting set in set-7.4.4
dpkg-source: info: unpacking set_7.4.4.orig.tar.gz
dpkg-source: info: unpacking set_7.4.4-0kali1.debian.tar.xz
dpkg-source: info: applying edit-config-file
dpkg-source: info: applying fix-path-interpreter.patch
$ wget https://github.com/trustedsec/social-engineer-toolkit/archive/7.4.5.tar.gz -O set_7.4.5.orig.tar.gz
[...]
$ tar xvf set_7.4.5.orig.tar.gz
[...]
social-engineer-toolkit-7.4.5/src/wireless/wifiattack.py
$ cp -a set-7.4.4/debian social-engineer-toolkit-7.4.5/debian
$ cd social-engineer-toolkit-7.4.5
$ dch -v 7.4.5-0buxy1 "New upstream release"
```

هذا هو. يمكنك الآن بناء الحزمة المحدثة.

اعتمادًا على نوع التغييرات التي يقدمها إصدار المصدر الجديد، قد تحتاج أيضًا إلى تغيير تبعيات البناء وتبعيات وقت التشغيل وتثبيت ملفات جديدة. هذه هي العمليات الأكثر مشاركة التي لم يشملها هذا الكتاب.

٤.١.٩. بدء البناء

عندما يتم تطبيق جميع التغييرات المطلوبة على المصادر، يمكنك البدء في إنشاء الحزمة الثنائية الفعلية أو ملف **deb**. تتم إدارة العملية برمتها بواسطة الأمر **dpkg-buildpackage** ويبدو كما يلي:

```
$ dpkg-buildpackage -us -uc -b
dpkg-buildpackage: source package libfreefare
dpkg-buildpackage: source version 0.4.0-2buxy1
dpkg-buildpackage: source distribution UNRELEASED
dpkg-buildpackage: source changed by Raphael Hertzog<buxy@kali.org>
dpkg-buildpackage: host architecture amd64
[...]
   dh_builddeb
dpkg-deb: building package 'libfreefare0-dbgsym' in '../libfreefare0-dbgsym_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: building package 'libfreefare0' in '../libfreefare0_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: building package 'libfreefare-dev' in '../libfreefare-dev_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: building package 'libfreefare-bin-dbgsym' in '../libfreefare-bin-dbgsym_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: building package 'libfreefare-bin' in '../libfreefare-bin_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: building package 'libfreefare-doc' in '../libfreefare-doc_0.4.0-2buxy1_all.deb'.
 dpkg-genchanges -b >../libfreefare_0.4.0-2buxy1_amd64.changes
dpkg-genchanges: binary-only upload (no source code included)
 dpkg-source --after-build libfreefare-0.4.0
dpkg-buildpackage: binary-only upload (no source included)
```

تعمل خيارات **uc-** **us-** على تعطيل التوقيعات على بعض الملفات التي تم إنشاؤها (**.dsc, .changes**) لأن هذه العملية ستفشل إذا لم يكن لديك مفتاح GnuPG مرتبط بالهوية التي وضعتها في ملف التغيير "change log" . يطلب خيار **b-** "بناء ثنائي فقط". في هذه الحالة، لن يتم إنشاء حزمة المصدر (**.dsc**)، سيتم إنشاء حزم (**.deb**) الثنائية فقط. استخدم هذا الخيار لتجنب الفشل أثناء بناء حزمة المصدر: إذا لم تكن قد سجلت تغييراتك بشكل صحيح في نظام إدارة التصحيح، فقد يشكو ويقاطع عملية البناء.

كما هو مقترح في رسائل **dpkg-deb**، فإن الحزم الثنائية التي تم إنشاؤها متاحة الآن في مجلد home (الذي يستضيف مجلد حزمة المصدر). يمكنك تثبيتها باستخدام **dpkg -i** أو **apt install**.

```
$ sudo apt install ../libfreefare0_0.4.0-2buxy1_amd64.deb
  ../libfreefare-bin_0.4.0-2buxy1_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libfreefare0' instead of '../libfreefare0_0.4.0-2buxy1_amd64.deb'
Note, selecting 'libfreefare-bin' instead of '../libfreefare-bin_0.4.0-2buxy1_amd64.deb'
The following packages will be upgraded:
  libfreefare-bin libfreefare0
```

2 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 0 B/69,4 kB of archives.

After this operation, 2 048 B of additional disk space will be used.

[...]

نفضل تثبيت **apt** على **dpkg -i**؛ لأنه سيتعامل مع التبعيات المفقودة بأمان. ولكن منذ وقت ليس ببعيد، كان عليك استخدام **dpkg** لأن **apt** لم يكن قادرًا على التعامل مع ملفات **.deb** خارج أي مستودع.

تغليف dpkg-buildpackage

غالبًا ما يستخدم مطورو دبيان برنامجًا عالي المستوى مثل: **debuild**؛ يعمل هذا على تشغيل **dpkg-buildpackage** كالمعتاد، ولكنه يضيف أيضًا استدعاء لبرنامج (**lintian**) يقوم بتشغيل العديد من عمليات التحقق للتحقق من صحة الحزمة التي تم إنشاؤها مقابل سياسة دبيان. يقوم هذا البرنامج النصي أيضًا بتنظيف البيئة بحيث لا تلوث متغيرات البيئة المحلية بنية الحزمة. يعد الأمر **debuild** أحد الأدوات الموجودة في مجموعة devscripts، والتي تشترك في بعض التناسق والتكوين لتسهيل مهمة المشرفين.

٢.٩. إعادة تجميع نواة لينكس

تشتمل النواة التي توفرها Kali على أكبر عدد ممكن من الميزات، بالإضافة إلى الحد الأقصى لعدد برامج التشغيل، من أجل تغطية أكبر مجموعة من تكوينات الأجهزة الموجودة. هذا هو السبب في أن بعض المستخدمين يفضلون إعادة ترجمة النواة من أجل تضمين ما يحتاجونه على وجه التحديد. هناك سببان لهذا الاختيار. أولاً، إنها طريقة لتحسين استهلاك الذاكرة حيث إن كل كود النواة، حتى لو لم يتم استخدامه أبدًا، يشغل الذاكرة الفعلية. نظرًا لأن:

الأجزاء المجمعة بشكل ثابت من النواة لا يتم نقلها مطلقًا لمساحة التبديل، فإن الانخفاض العام في أداء النظام سينتج عن وجود برامج تشغيل وميزات مدمجة لا يتم استخدامها مطلقًا.

ثانيًا: يؤدي تقليل عدد برامج التشغيل وميزات النواة إلى تقليل مخاطر حدوث مشكلات أمنية، نظرًا لأنه لا يتم تشغيل سوى جزء صغير من كود النواة المتاح.

مهم

إذا اخترت تجميع النواة الخاصة بك، يجب عليك قبول العواقب: لا يمكن لـ Kali ضمان تحديثات الأمان للنواة المخصصة الخاصة بك. من خلال الحفاظ على النواة التي قدمها كالي، يمكنك الاستفادة من التحديثات التي أعدها مشروع ديبان.

إعادة تجميع النواة ضروري أيضًا إذا كنت ترغب في استخدام ميزات معينة متوفرة فقط كـ patches (وغير مضمنة في إصدار النواة القياسي).

دليل نواة ديبان

يحافظ فريق نواة Debian على دليل Debian Kernel (متوفر أيضًا في حزمة debian-kernel-handbook) مع وثائق شاملة حول معظم المهام المتعلقة بالنواة وحول كيفية معالجة حزم Debian kernel الرسمية. هذا هو المكان الأول الذي يجب أن تبحث فيه إذا كنت بحاجة إلى مزيد من المعلومات أكثر مما هو متوفر في هذا القسم.
http://kernel-handbook.alioth.debian.org

١.٢.٩. مقدمة ومتطلبات مسبقة

من غير المستغرب أن يدير ديبيان وكالي النواة في شكل حزمة، وهي ليست الطريقة التي تم بها تجميع النواة وتثبيتها تقليديًا. بما أن النواة تظل تحت سيطرة نظام التغليف، فيمكن بعد ذلك إزالتها بشكل نظيف أو نشرها على عدة أجهزة. علاوة على ذلك، تعمل البرامج النصية المرتبطة بهذه الحزم على أتمتة التفاعل مع أداة تحميل التشغيل والمولد الأول.

تحتوي مصادر لينكس الأولية على كل ما يلزم لبناء حزمة دبيان من النواة ولكنك ما زلت بحاجة إلى تثبيت حزمة البناء الأساسية للتأكد من أن لديك الأدوات اللازمة لبناء حزمة دبيان. علاوة على ذلك، تتطلب خطوة التكوين للنواة حزمة libncurses5-dev. أخيرًا، ستتيح حزمة fakeroot إنشاء حزمة دبيان دون الحاجة إلى امتيازات إدارية.

```
# apt install build-essential libncurses5-dev fakeroot
```

٢.٢.٩. الحصول على المصادر

بما أن مصادر نواة لينكس متوفرة كحزمة، يمكنك استعادتها عن طريق تثبيت حزمة linux-source-*version*. يجب أن يسرد الأمر **apt-cache search ^linux-source** أحدث إصدار من النواة تم تعبئته بواسطة Kali. لاحظ أن كود المصدر الموجود في هذه الحزم لا تتوافق بدقة مع تلك التي نشرها لينوس تورفالدس ومطورو النواة؛ مثل جميع التوزيعات، يطبق ديبيان وكالي عدداً من التصحيحات، والتي (أو قد لا) تجد طريقها إلى الإصدار الأعلى من لينكس. تتضمن هذه التعديلات منافذ خلفية للإصلاحات/الميزات/ برامج التشغيل من إصدارات النواة الأحدث، وميزات جديدة لم يتم دمجها بعد (بالكامل) في شجرة Linux upstream، وأحياناً حتى تغييرات خاصة بـ Debian أو Kali.

يركز الجزء المتبقي من هذا القسم على الإصدار ٩.٤ من نواة لينكس، ولكن يمكن بالطبع تكييف الأمثلة مع الإصدار المحدد من النواة التي تريدها.

في هذا المثال، نفترض أنه تم تثبيت الحزمة الثنائية linux-source-4.9. لاحظ أننا نقوم بتثبيت حزمة ثنائية تحتوي على مصادر المصدر ولكن لا نقوم باسترداد حزمة مصدر Kali المسماة linux.

```
# apt install linux-source-4.9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
```

```
  bc libreadline7
Suggested packages:
  libncurses-dev | ncurses-dev libqt4-dev
The following NEW packages will be installed:
  bc libreadline7 linux-source-4.9
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 95.4 MB of archives.
After this operation, 95.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
[...]
```

```
# ls /usr/src
linux-config-4.9        linux-patch-4.9-rt.patch.xz
linux-source-4.9.tar.xz
```

٣.٢.٩. تكوين النواة

تتكون الخطوة التالية من تكوين النواة وفقًا لاحتياجاتك. يعتمد الإجراء الدقيق على الأهداف.

يعتمد بناء النواة على ملف تكوين النواة. في معظم الحالات، ستبقى على الأرجح قريبًا قدر الإمكان من تلك التي اقترحها Kali، والتي، مثل جميع توزيعات Linux، مثبتة في مجلد **/boot**. في هذه الحالة، بدلاً من إعادة تكوين كل شيء من البداية، يكفي عمل نسخة من ملف **/boot/config-***version*. (يجب أن يكون الإصدار هو نفس إصدار النواة المستخدمة حاليًا، والذي يمكن العثور عليه باستخدام الأمر **uname -r**) ضع النسخة في ملف **config**. في المجلد الذي يحتوي على مصادر النواة.

```
$ cp /boot/config-4.9.0-kali1-amd64 ~/kernel/linux-source-4.9/.config
```

بدلاً من ذلك، نظراً لأن النواة توفر تكوينات افتراضية في **arch/***arch***/configs/*_defconfig**، يمكنك وضع التكوين المحدد في مكانه باستخدام أمر مثل **make x86_64_defconfig** (في حالة جهاز حاسوب ذي بنية 64bit) أو **make i386_defconfig** (في حالة جهاز حاسوب ذي بنية 32bit).

ما لم تكن بحاجة إلى تغيير التكوين، يمكنك التوقف هنا والانتقال إلى القسم ٤.٢.٩، "تجميع وبناء الحزمة". إذا كنت بحاجة إلى إجراء تغييرات أو إذا قررت إعادة تكوين كل شيء من البداية، يجب أن تأخذ الوقت الكافي لتكوين نواة الخاص بك. هناك العديد من الواجهات المخصصة في دليل مصدر النواة والتي يمكن استخدامها عن طريق استدعاء الأمر **make** *target*، حيث يمثل الهدف إحدى القيم الموضحة أدناه.

make menuconfig يجمع ويطلق واجهة تكوين النواة في وضع النص (هذا هو المكان الذي نتطلب حزمة libncurses5-dev)، مما يسمح بالتنقل في العديد من خيارات النواة المتاحة في الهيكل الهرمي. يؤدي الضغط على مفتاح **Space** إلى تغيير قيمة الخيار المحدد، و **Enter** للتحقق من الزر المحدد أسفل الشاشة؛ **Select** يرجع إلى القائمة الفرعية المحددة؛ **Exit** يغلق الشاشة الحالية وينتقل مرة أخرى في التسلسل الهرمي. ستعرض **Help** معلومات أكثر تفصيلاً حول دور الخيار المحدد. تسمح مفاتيح الأسهم بالتحرك ضمن قائمة الخيارات والأزرار. للخروج من برنامج التكوين، اختر **Exit** من القائمة الرئيسية. ثم يعرض البرنامج لحفظ التغييرات التي أجريتها؛ تقبل إذا كنت راضياً عن اختياراتك.

تحتوي واجهات أخرى على ميزات متشابهة ولكنها تعمل ضمن واجهات رسومية أكثر حداثة، مثل **make xconfig**، الذي يستخدم واجهة رسومية Qt، و**make gconfig**، والذي يستخدم +GTK. يتطلب الأول libqt4-dev، بينما يعتمد الأخير على libglade2-dev و -libgtk2.0 dev.

التعامل مع ملفات config. القديمة

عند تقديم ملف **config.** تم إنشاؤه باستخدام إصدار نواة آخر (عادةً أقدم)، يجب عليك تحديثه. يمكنك القيام بذلك باستخدام **`make oldconfig`**، والذي سيسألك بشكل تفاعلي الأسئلة المقابلة لخيارات التكوين الجديدة. إذا كنت ترغب في استخدام الإجابة الافتراضية لجميع هذه الأسئلة، يمكنك استخدام **`make olddefconfig`**. بـ **`make oldnoconfig`**، ستفترض إجابة سلبية على جميع الأسئلة.

٤.٢.٩. تجميع وبناء الحزمة

تنظيف قبل إعادة البناء

إذا كنت قد قمت بالفعل بتجميع نواة في المجلد وترغب في إعادة بناء كل شيء من البداية (على سبيل المثال لأنك قمت بتغيير تكوين النواة بشكل كبير)، فسيتعين عليك تشغيل **make clean** لإزالة الملفات المترجمة. يؤدي إجراء **make distclean** لإزالة المزيد من الملفات التي تم إنشاؤها، بما في ذلك ملف **config.**، لذا تأكد من نسخه احتياطيًا أولاً.

بمجرد أن يصبح تكوين النواة جاهزًا، ستؤدي عملية **make deb-pkg** البسيطة إلى إنشاء ما يصل إلى خمس حزم Debian بتنسيق **deb.** القياسي: linux-image-*version*، والتي تحتوي على صورة النواة والوحدات المرتبطة بها؛ linux-headers-*version*، الذي يحتوي على ملفات الرأس المطلوبة لبناء وحدات خارجية؛ linux-firmware-image-version، الذي يحتوي على ملفات البرامج الثابتة التي تحتاجها بعض برامج التشغيل (قد تكون هذه الحزمة مفقودة عند الإنشاء من مصادر النواة التي توفرها Debian أو Kali)؛ linux-image-version-dbg، الذي يحتوي على رموز التصحيح لصورة النواة ووحداتها؛ و linux-libc-dev، الذي يحتوي على رؤوس ذات صلة ببعض مكتبات مساحة المستخدم مثل مكتبة سي جنو (glibc).

يتم تعريف الإصدار من خلال تسلسل إصدار المصدر (كما هو محدد بواسطة المتغيرات VERSION و PATCHLEVEL و SUBLEVEL و EXTRAVERSION في Makefile)،

ومعلمة التكوين **LOCALVERSION**، ومتغير البيئة LOCALVERSION. يستخدم إصدار الحزمة نفس سلسلة الإصدار مع مراجعة ملحقة يتم زيادتها بانتظام (وتخزينها في **version.**) ، إلا إذا تجاوزتها مع متغير البيئة **KDEB_PKGVERSION**.

```
$ make deb-pkg LOCALVERSION=-custom KDEB_PKGVERSION=$(make kernelversion)-1
[...]
$ ls ../*.deb
../linux-headers-4.9.0-kali1-custom_4.9.2-1_amd64.deb
../linux-image-4.9.0-kali1-custom_4.9.2-1_amd64.deb
../linux-image-4.9.0-kali1-custom-dbg_4.9.2-1_amd64.deb
../linux-libc-dev_4.9.2-1_amd64.deb
```

لاستخدام النواة المدمجة بالفعل، فإن الخطوة الوحيدة المتبقية هي تثبيت الحزم المطلوبة بـ **dpkg -i** *file.deb*. حزمة الـ "linux-image" مطلوبة؛ ما عليك سوى تثبيت حزمة "linux-headers" إذا كان لديك بعض وحدات النواة الخارجية المطلوب إنشاؤها، وهذا هو الحال إذا كان لديك بعض حزم "dkms-*" مثبتة (راجع **dpkg -l "*-dkms" | grep ^ii**). لا تحتاج الحزم الأخرى بشكل عام (إلا إذا كنت تعرف لماذا تحتاجها!).

٣.٩. بناء صور ISO مخصصة لكالي مباشر

يتمتع Kali Linux بالكثير من الوظائف والمرونة. بمجرد تثبيت Kali، يمكنك أداء جميع أنواع الأعمال المذهلة مع القليل من التوجيه والإبداع والصبر والممارسة. ومع ذلك، يمكنك أيضًا تخصيص إصدار Kali بحيث يحتوي على ملفات أو حزم محددة (لزيادة الأداء والميزات أو تقليصها) ويمكنه أداء وظائف معينة تلقائيًا. على سبيل المثال، يعد كل من Kali ISO لـ Doom و Kali Evil Wireless Access Point مشاريع ممتازة تعتمد على تنفيذ مصمم خصيصًا لـ Kali Linux. دعونا نلقي نظرة على عملية طرح صورة مخصصة لـ Kali Linux ISO.

تم إنشاء صور Kali ISO الرسمية ببناء مباشر، وهو عبارة عن مجموعة من البرامج النصية التي تتيح الأتمتة والتخصيص الكامل لجميع جوانب إنشاء صورة ISO. يستخدم خيار البناء المباشر بنية دليل كاملة كمدخل لتكوينه. نقوم بتخزين هذا التكوين وبعض البرامج النصية المساعدة المرتبطة في مستودع Git للبناء المباشر. سنستخدم هذا المستودع كأساس لبناء صور مخصصة.

قبل المضي قدمًا، يجب أن تعرف أن الأوامر الموضحة في هذا القسم مخصصة للتشغيل على نظام Kali Linux حديث. من المحتمل جدًا أن تفشل إذا تم تشغيلها على نظام غير كالي أو إذا كان النظام قديمًا.

١.٣.٩. تثبيت المتطلبات المسبقة

الخطوة الأولى هي تثبيت الحزم المطلوبة واسترجاع مستودع Git مع تكوين Kali للبناء المباشر:

```
# apt install curl git live-build
[...]

# git clone git://gitlab.com/kalilinux/build-scripts/live-build-config.git
[...]

# cd live-build-config
# ls
auto  build_all.sh  build.sh  kali-config  README
```

عند هذه النقطة، يمكنك بالفعل إنشاء صورة محدثة (ولكن غير معدلة) لـ Kali ISO فقط عن طريق تشغيل **./build.sh --verbose**. سيستغرق البناء وقتًا طويلاً حتى يكتمل حيث سيتم تنزيل جميع الحزم لتضمينها. عند الانتهاء، ستجد صورة ISO الجديدة في مجلد **images**.

٢.٣.٩. بناء صور مباشرة مع بيئات سطح المكتب المختلفة

يعد برنامج البناء المباشر build.sh الذي نقدمه مسؤولاً عن إعداد مجلد **config** الذي يتوقع الإنشاء المباشر العثور عليه. يمكنها وضع تكوينات مختلفة اعتمادًا على خيارها **--variant**.

ينشئ التغليف مجلد **config** من خلال دمج الملفات من **kali-config/common** و **kali-config/variant-*X***، حيث X هو اسم متغير مع المعلمة **--variant**. عندما لا يكون الخيار محددًا بشكل صريح، فإنه يستخدم الإعداد الافتراضي "**default**" كاسم المتغير.

يحتوي مجلد **kali-config** على مجلدات لبيئات سطح المكتب الأكثر شيوعًا:

- **e17** for Enlightenment;
- **gnome** for GNOME;
- **i3wm** for the corresponding window manager;
- **kde** for KDE;
- **lxde** for LXDE;
- **mate** for the Mate Desktop Environment;
- **xfce** for XFCE.

متغير **light** خاص قليلاً، وهو يعتمد على XFCE ويستخدم لإنشاء صور ISO "الخفيفة" الرسمية التي تحتوي على مجموعة مخفضة من التطبيقات.

يمكنك بسهولة إنشاء صورة مباشرة لـ Kali باستخدام KDE كبيئة سطح مكتب باستخدام هذا الأمر:

```
# ./build.sh --variant kde --verbose
```

يسمح مفهوم المتغير هذا ببعض التخصيصات عالية المستوى المحددة مسبقًا ولكن إذا خصصت بعض الوقت لقراءة دليل نظام Debian Live System، فسوف تكتشف العديد من الطرق الأخرى لتخصيص الصور، فقط عن طريق تغيير محتوى الجزء الفرعي المناسب مجلد تكوين كالي. ستقدم الأقسام التالية بعض الأمثلة.

٣.٣.٩. تغيير مجموعة الحزم المثبتة

بمجرد إطلاقه، يقوم الإصدار المباشر بتثبيت جميع الحزم المدرجة في ملفات .* / package-list list.chroot. يتضمن التكوين الافتراضي الذي نقدمه ملف package-قوائم / kali.list.chroot ، والذي يسرد kali-linux-full (الحزمة الوصفية الرئيسية التي تسحب جميع حزم Kali لتضمينها). يمكنك التعليق على هذه الحزمة ووضع حزمة تعريفية أخرى من اختيارك أو تضمين مجموعة دقيقة من الحزم الأخرى. يمكنك أيضًا الجمع بين كلا النهجين من خلال البدء بحزمة تعريف وإضافة حزم تكميلية من اختيارك.

مع **package-lists**، يمكنك فقط تضمين الحزم المتوفرة بالفعل في مستودع Kali الرسمي. ولكن إذا كان لديك حزم مخصصة، يمكنك تضمينها في الصورة المباشرة عن طريق وضع ملفات **deb.** في مجلد **packages.chroot** (على سبيل المثال **kali-config/config-gnome/packages.chroot** إذا قمت بإنشاء متغير جنوم).

الحزم التعريفية عبارة عن حزم فارغة هدفها الوحيد الحصول على العديد من التبعيات على الحزم الأخرى. إنها تجعل من السهل تثبيت مجموعات الحزم التي غالبًا ما ترغب في تثبيتها معًا. تقوم حزمة مصدر kali-meta ببناء جميع الحزم الوصفية التي تقدمها Kali Linux:

kali-linux: النظام الأساسي (يتم سحبه بواسطة جميع الحزم التعريفية الأخرى)

kali-linux-full: التثبيت الافتراضي لـ Kali Linux

kali-linux-all: الحزمة الوصفية لجميع الحزم التعريفية والحزم الأخرى (تقريبًا كل ما توفره Kali لذلك فهي ضخمة حقًا!)

kali-linux-sdr: أدوات الراديو المعرفة بالبرمجيات (SDR) "Software Defined Radio"

kali-linux-gpu: أدوات مدعومة بمعالج الجرافيكس (أدوات تستخدم قوة الحوسبة المتوفرة في بطاقتك الرسومية)

kali-linux-wireless: أدوات التقييم والتحليل اللاسلكية

kali-linux-web: أدوات تقييم تطبيقات الويب

kali-linux-forensic: أدوات التحقيق الجنائي (إيجاد دليل على ما حدث)

kali-linux-voip: أدوات Voice Over IP

kali-linux-pwtools: أدوات تكسير كلمة المرور

kali-linux-top10: الأدوات العشرة الأكثر شعبية

kali-linux-rfid: أدوات RFID

يمكنك الاستفادة من هذه الحزم الوصفية عند إنشاء قوائم حزم مخصصة للبناء المباشر. يمكن الاطلاع على القائمة الكاملة للحزم التعريفية والأدوات التي تتضمنها على http://tools.kali.org/kali-metapackages

Debconf توقع الحزم المثبتة

يمكنك تقديم ملفات **Debconf** المتوقعة (انظر القسم ٢.٣.٤، "إنشاء ملف **Preseed**" للحصول على تفسيرات) كملفات **preseed/*.cfg**. سيتم استخدامها لتكوين الحزم المثبتة في نظام الملفات المباشر.

٤.٣.٩. استخدام الخطافات "hooks" لتعديل محتويات الصورة

يقدم البناء المباشر خطافات يمكن تنفيذها في خطوات مختلفة من عملية البناء. الخطافات Chroot هي برامج نصية قابلة للتنفيذ تقوم بتثبيتها كملفات **hooks/live/*.chroot** في شجرة التكوين الخاصة بك والتي يتم تنفيذها داخل chroot. على الرغم من أن chroot هو الأمر الذي يتيح لك تغيير مجلد الجذر لنظام التشغيل مؤقتًا إلى مجلد من اختيارك، فإنه يستخدم أيضًا عن طريق الإضافة لتعيين مجلد يستضيف شجرة نظام ملفات (بديلة) كاملة. هذا هو الحال هنا مع الإنشاء المباشر، حيث يكون مجلد chroot هو المجلد الذي يتم فيه تحضير نظام الملفات الحية. نظراً لأن التطبيقات التي تم بدء تشغيلها في chroot لا يمكن رؤيتها خارج هذا المجلد، فإن الأمر نفسه ينطبق على عمليات خطاف chroot: يمكنك فقط استخدام وتعديل أي شيء متاح في بيئة chroot. نحن نعتمد على تلك الخطافات لإجراء العديد من التخصيصات الخاصة بـ Kali (انظر **kali-config/common/hooks/live/kali-hacks.chroot**).

يتم تنفيذ الخطافات الثنائية (**hooks/live/*.binary**) في سياق عملية البناء (ولا يتم جذرها "chrooted" في أي مكان) في نهاية العملية. يمكنك تعديل محتوى صورة ISO التي تم إنشاؤها ولكن ليس لنظام الملفات المباشرة، حيث تم إنشاؤها بالفعل في هذه المرحلة. نستخدم هذه الميزة في كالي لإجراء بعض التغييرات على التكوين المعزول الافتراضي الناتج عن البناء المباشر. على سبيل المثال، راجع **kali-config/common/hooks/live/persistence.binary** حيث نضيف إدخالات قائمة الإقلاع لتمكين الثبات"persistence".

٥.٣.٩. إضافة ملفات في صورة ISO أو في نظام الملفات المباشر

التخصيص الشائع الآخر هو إضافة الملفات إما في نظام الملفات المباشر أو في صورة ISO.

يمكنك إضافة ملفات إلى نظام الملفات المباشر عن طريق وضعها في موقعها المتوقع تحت مجلد **includes.chroot**. على سبيل المثال، نقدم:

kali-config/common/includes.chroot/usr/lib/live/config/0031-root-password

والذي ينتهي بـ: **/usr/lib/live/config/0031-root-password** في نظام الملفات المباشر.

خطاف الإقلاع المباشر

يتم تنفيذ البرامج النصية المثبتة كـ **/lib/live/config/***XXXX-name* بواسطة البرنامج النصي init لحزمة الإقلاع المباشر. تكوين العديد من الجوانب للنظام لتكون مناسبة لنظام مباشر. يمكنك إضافة نصوص برمجية خاصة بك لتخصيص نظامك المباشر في وقت التشغيل: يتم استخدامه بشكل خاص لتنفيذ معلمة الإقلاع مخصصة على سبيل المثال.

يمكنك إضافة ملفات لصورة ISO بوضعها في موقعها المتوقع تحت مجلد التكوين **includes.binary**. على سبيل المثال، نحن نقدم:

kali-config/common/includes.binary/isolinux/splash.png

لتجاوز صورة الخلفية التي يستخدمها محمل الإقلاع Isolinux (الذي يتم تخزينه في **/isolinux/splash.png** في نظام ملفات صورة ISO).

٤.٩. إضافة الثبات إلى ISO المباشر باستخدام مفتاح USB

١.٤.٩. ميزة الثبات: توضيح

بعد ذلك، سنناقش الخطوات المطلوبة لإضافة الثبات لمفتاح Kali USB. طبيعة النظام المباشر هي أن تكون سريعة الزوال. يتم فقدان جميع البيانات المخزنة على النظام المباشر وجميع التغييرات التي تم إجراؤها عند إعادة التشغيل. لعلاج هذا، يمكنك استخدام ميزة الإقلاع المباشر تسمى الثبات "**persistence**"، والتي يتم تمكينها عندما تتضمن معلمات الإقلاع الكلمة الأساسية الثبات "**persistence**".

نظراً لأن تعديل قائمة الإقلاع يعد مهمة غير تافهة، فإن Kali يتضمن إدخالين للقائمة بشكل افتراضي لتمكين الثبات: Live USB Persistence و Live USB Encrypted Persistent، كما هو موضح في الشكل ١.٩، "خيارات النظام المباشر الثابت".



شكل ١.٩، "خيارات النظام المباشر الثابت"

عند تمكين هذه الميزة، سيفحص الإقلاع المباشر جميع الأقسام التي تبحث عن أنظمة الملفات التي تحمل علامة Persistence (والتي يمكن تجاوزها بمعلمة الإقلاع **persistence-label**=*value*) وسيعمل المثبت على إعداد ثبات المجلدات المدرجة في ملف **persistence.conf** الموجود في هذا القسم (مجلد واحد لكل سطر). تتيح القيمة الخاصة "**/union**" الثبات الكامل لجميع المجلدات من خلال *union mount*، وهو تراكب يخزن التغييرات فقط عند مقارنتها بنظام الملفات الأساسي. يتم تخزين بيانات المجلدات الثابتة في نظام الملفات الذي يحتوي على ملف **persistence.conf** المقابل.

٢.٤.٩. إعداد ثبات غير مشفر على مفتاح USB

في هذا القسم، نفترض أنك أعددت مفتاح Kali Live USB باتباع الإرشادات الواردة في القسم ٢,١,٤، "نسخ الصورة على قرص DVD أو مفتاح USB" وأنك استخدمت مفتاح USB كبيرًا بما يكفي لاستيعاب صورة ISO (حوالي ٣ غيغابايت) وبيانات المجلدات التي تريد ثباتها. نفترض أيضًا أن نظام USB يتم التعرف عليه من خلال Linux كـ **dev/sdb/** وأنه يحتوي فقط على القسمين اللذين يمثلان جزءًا من صورة ISO الافتراضية (**dev/sdb1/** و **dev/sdb2/**). كن حذرا للغاية عند تنفيذ هذا الإجراء. يمكنك بسهولة تدمير البيانات المهمة إذا قمت بإعادة تقسيم محرك الأقراص الخاطئ.

لإضافة قسم جديد، يجب أن تعرف حجم الصورة التي نسختها حتى تتمكن من جعل القسم الجديد يبدأ بعد الصورة الحية. ثم استخدم **parted** لإنشاء القسم بالفعل. تبين الأوامر التالية صورة ISO المسماة kali-linux-2016.1-amd64.iso، والتي يُفترض أنها موجودة على مفتاح USB أيضًا:

```
# parted /dev/sdb print
Model: SanDisk Cruzer Edge (scsi)
Disk /dev/sdb: 32,0GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
 1      32,8kB  2852MB  2852MB  primary               boot, hidden
 2      2852MB  2945MB  93,4MB  primary
```

```
# start=$(du --block-size=1MB kali-linux-2016.1-amd64.iso | awk '{print $1}')

# echo "Size of image is $start MB"
Size of image is 2946 MB

# parted -a optimal /dev/sdb mkpart primary "${start}MB" 100%
Information: You may need to update /etc/fstab.


# parted /dev/sdb print
Model: SanDisk Cruzer Edge (scsi)
Disk /dev/sdb: 32,0GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
 1           32,8kB    2852MB    2852MB    primary  boot, hidden
 2      2852MB  2945MB  93,4MB  primary
 3      2946MB  32,0GB  29,1GB  primary
```

مع وجود قسم **dev/sdb3/** الجديد، قم بتهيئته بنظام ملفات **ext4** المسمى "persistence" بمساعدة الأمر **mkfs.ext4** (وخياره **L-** لتعيين التسمية). يتم بعد ذلك تحميل القسم على المجلد **mnt/** ثم تقوم بإضافة ملف التكوين **persistence.conf** المطلوب. كالعادة، كن حذرًا عند تنسيق أي قرص. قد تفقد معلومات قيمة إذا قمت بتهيئة القرص أو القسم الخطأ.

```
# mkfs.ext4 -L persistence /dev/sdb3
mke2fs 1.43-WIP (15-Mar-2016)
Creating filesystem with 7096832 4k blocks and 1777664 inodes
Filesystem UUID: dede20c4-5239-479a-b115-96561ac857b6
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632,
2654208,
     4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
# mount /dev/sdb3 /mnt
# echo "/ union" >/mnt/persistence.conf

# ls -l /mnt
total 20
drwx------ 2 root root 16384 May 10 13:31 lost+found
-rw-r--r-- 1 root root     8 May 10 13:34 persistence.conf
# umount /mnt
```

مفتاح USB جاهز الآن ويمكن تشغيله بالاختيار من قائمة الإقلاع "Live USB Persistent".

٣.٤.٩. إعداد الثبات المشفر على مفتاح USB

الإقلاع المباشر قادر أيضًا على التعامل مع أنظمة الملفات الثابتة على الأقسام المشفرة. وبالتالي يمكنك حماية بيانات المجلدات الدائمة الخاصة بك عن طريق إنشاء قسم مشفر LUKS يحتوي على بيانات الثبات.

الخطوات الأولية هي نفسها لإنشاء القسم ولكن بدلاً من تنسيقه باستخدام نظام ملفات **ext4**، استخدم **cryptsetup** لتهيئته كحاوية LUKS. ثم افتح تلك الحاوية وقم بإعداد نظام الملفات **ext4** بنفس الطريقة كما في الإعداد غير المشفر، ولكن بدلاً من استخدام قسم **/dev/sdb3**، استخدم القسم الافتراضي الذي تم إنشاؤه بواسطة **cryptsetup**. يمثل هذا القسم الافتراضي المحتوى الذي تم فك تشفيره للقسم المشفر، والذي يتوفر في **/dev/mapper** تحت الاسم الذي قمت بتعيينه له. في المثال أدناه، سنستخدم اسم **kali_persstanding**. مرة أخرى، تأكد من أنك تستخدم محرك الأقراص والقسم الصحيحين.

```
# cryptsetup --verbose --verify-passphrase luksFormat /dev/sdb3

WARNING!
========
This will overwrite data on /dev/sdb3 irrevocably.
Are you sure? (Type uppercase yes): YES
Enter passphrase:
Verify passphrase:
Command successful.
```

```
# cryptsetup luksOpen /dev/sdb3 kali_persistence
Enter passphrase for /dev/sdb3:
# mkfs.ext4 -L persistence /dev/mapper/kali_persistence
mke2fs 1.43-WIP (15-Mar-2016)
Creating filesystem with 7096320 4k blocks and 1774192 inodes
Filesystem UUID: 287892c1-00bb-43cb-b513-81cc9e6fa72b
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

# mount /dev/mapper/kali_persistence /mnt
# echo "/ union" >/mnt/persistence.conf
# umount /mnt
# cryptsetup luksClose /dev/mapper/kali_persistence
```

٤.٤.٩. استخدام مخازن الثبات المتعددة

إذا كان لديك العديد من حالات الاستخدام لنظام Kali المباشر الخاص بك، يمكنك استخدام أنظمة ملفات متعددة ذات تصنيفات مختلفة والإشارة في سطر أوامر الإقلاع إلى (set of) أنظمة الملفات التي يجب استخدامها لميزة الثبات: يتم ذلك بمساعدة معلمة الإقلاع **persistence-label**=*label*.

لنفترض أنك محترف اختبار اختراق. عندما تعمل لدى أحد العملاء، فإنك تستخدم قسمًا ثابتًا مشفراً لحماية سرية بياناتك في حالة سرقة مفتاح USB أو اختراقه. في الوقت نفسه، تريد أن تكون قادرًا على عرض Kali وبعض المواد الترويجية المخزنة في قسم غير مشفر من مفتاح USB نفسه. نظرًا لأنك لا تريد تعديل معلمات الإقلاع يدويًا في كل إلاقلاع، فأنت تريد إنشاء صورة مباشرة مخصصة مع إدخالات قائمة تشغيل مخصصة.

تتمثل الخطوة الأولى في إنشاء ISO مباشر مخصص (بعد القسم ٩,٣، "إنشاء صور ISO مخصصة لـ Kali Live" وخاصة القسم ٩,٣,٤، "استخدام الخطافات لتعديل محتويات الصورة"). التخصيص الرئيسي هو تعديل **kali-config/common/hooks/live/persistence-menu.binary** لجعله يبدو مثل هذا (لاحظ معلمات **persistence-label**):

```
#!/bin/sh
if [ ! -d isolinux ]; then
    cd binary
fi
cat >>isolinux/live.cfg <
```

بعد ذلك، سنقوم ببناء ISO المخصص الخاص بنا ونسخه إلى مفتاح USB. ثم سنقوم بإنشاء وتهيئة القسمين والملفات التي سيتم استخدامها للثبات. القسم الأول غير مشفر (المسمى "demo")، والثاني مشفر (المسمى "work"). بافتراض **dev/sdb/** هو مفتاح USB الخاص بنا وحجم صورة ISO المخصصة لدينا ٣٠٠٠ ميجا بايت، سيبدو كما يلي:

```
# parted /dev/sdb mkpart primary 3000 MB 55%
# parted /dev/sdb mkpart primary 55% 100%
# mkfs.ext4 -L demo /dev/sdb3
[...]
# mount /dev/sdb3 /mnt
# echo "/ union" >/mnt/persistence.conf
# umount /mnt
#    cryptsetup    --verbose    --verify-passphrase
luksFormat /dev/sdb4
[...]
# cryptsetup luksOpen /dev/sdb4 kali_persistence
[...]
# mkfs.ext4 -L work /dev/mapper/kali_persistence
[...]
# mount /dev/mapper/kali_persistence /mnt
# echo "/ union" >/mnt/persistence.conf
# umount /mnt
# cryptsetup luksClose /dev/mapper/kali_persistence
```

وهذا كل شيء. يمكنك الآن تشغيل مفتاح USB والاختيار من إدخالات قائمة الإقلاع الجديدة حسب الحاجة!

إضافة كلمة مرور Nuke لمزيد من الأمان

يوفر Kali حزمة cryptsetup-nuke-password التي تعدل البرنامج النصي **cryptsetup** لتطبيق ميزة جديدة: يمكنك تعيين كلمة مرور nuke والتي - عند استخدامها - ستدمر جميع المفاتيح المستخدمة لإدارة القسم المشفر.

يمكن أن يكون هذا مفيدًا عندما تسافر كثيرًا وتحتاج إلى طريقة سريعة لضمان عدم استعادة بياناتك. عند الإقلاع، فقط اكتب كلمة مرور nuke بدلاً من كلمة المرور الحقيقية، ومن ثم سيكون من المستحيل على أي شخص (بما في ذلك أنت) الوصول إلى بياناتك.

قبل استخدام هذه الميزة، من الحكمة إنشاء نسخة احتياطية من مفاتيح التشفير الخاصة بك والاحتفاظ بها في مكان آمن.

يمكنك تكوين كلمة مرور nuke باستخدام هذا الأمر (بافتراض تثبيت الحزمة):

```
$ dpkg-reconfigure cryptsetup-nuke-password
```

يمكن العثور على مزيد من المعلومات حول هذه الميزة في البرنامج التعليمي التالي:

https://www.kali.org/tutorials/nuke-kali-linux-luks/

٥.٩. ملخص

تعلمنا في هذا الفصل كيفية تعديل حزم مصدر Kali، والتي تعد اللبنات الأساسية لجميع التطبيقات التي يتم شحنها في Kali. اكتشفنا أيضًا كيفية تخصيص نواة Kali وتثبيتها. ثم ناقشنا بيئة البناء المباشر وناقشنا كيفية إنشاء صورة Kali Linux ISO مخصصة. لقد أظهرنا أيضًا كيفية إنشاء عمليات تثبيت Kali USB مشفرة وغير مشفرة.

١.٥.٩. نصائح موجزة لتعديل حزم كالي

عادة ما يكون تعديل حزم Kali مهمة للمساهمين والمطورين في Kali، ولكن قد يكون لديك احتياجات محددة لم يتم تلبيتها من خلال الحزم الرسمية ومعرفة كيفية بناء حزمة معدلة يمكن أن يكون مفيدًا للغاية، خاصة إذا كنت ترغب في مشاركة تغييراتك، فقم بنشرها داخليًا، أو أعد البرنامج إلى الحالة السابقة.

عندما تحتاج إلى تعديل جزء من البرنامج، فقد يكون من المغري تنزيل المصدر وإجراء التغييرات واستخدام البرنامج المعدل. ومع ذلك، إذا كان تطبيقك يتطلب إعدادًا على مستوى النظام (على سبيل المثال بخطوة التثبيت)، فسوف يلوث نظام الملفات الخاص بك بالملفات غير المعروفة لـ **dpkg** وسيؤدي قريبًا إلى حدوث مشكلات لا يمكن اكتشافها من خلال تبعيات الحزمة. بالإضافة إلى ذلك، فإن هذا النوع من تعديل البرنامج ممل للمشاركة.

عند إنشاء حزمة معدلة، تكون العملية العامة هي نفسها دائمًا: احصل على الحزمة المصدر، واستخرجها، وأدخل التغييرات، ثم أنشئ الحزمة. لكل خطوة، غالبًا ما تكون هناك أدوات متعددة يمكنها التعامل مع كل مهمة.

لبدء إعادة بناء حزمة Kali، قم أولاً بتنزيل الحزمة المصدر، والتي تتكون من ملف **dsc.*** (التحكم في مصدر دبيان) وملفات إضافية تمت الإشارة إليها من ملف التحكم هذا.

يتم تخزين حزم المصدر على المرايا التي يمكن الوصول إليها عبر بروتوكول HTTP. الطريقة الأكثر فعالية للحصول عليها هي **apt source** *source-package-name*، الأمر الذي يتطلب منك إضافة سطر **deb-src** إلى ملف **/etc/apt/sources.list** وتحديث ملفات الفهرس بـ **apt update**.

بالإضافة إلى ذلك، يمكنك استخدام **dget** (من حزمة devscripts) لتنزيل ملف **dsc.** مباشرة مع الملفات المرفقة به. بالنسبة إلى الحزم الخاصة بـ Kali التي تتم استضافة مصادرها في مستودع Git على **gitlab.com/kalilinux**، يمكنك استرداد المصادر باستخدام:

```
git clone git://gitlab.com/kalilinux/packages/source-package
```

(إذا كنت لا ترى أي شيء في المستودع الخاص بك، حاول التبديل إلى فرع **kali/master** مع **git checkout kali/master**).

بعد تنزيل المصادر، قم بتثبيت الحزم المدرجة في تبعيات بناء الحزمة المصدر باستخدام **sudo apt build-dep ./**. يجب تشغيل هذا الأمر من مجلد مصدر الحزمة.

تتكون تحديثات حزمة المصدر من مجموعة من الخطوات التالية:

الخطوة الأولى المطلوبة هي تغيير رقم الإصدار لتمييز الحزمة الخاصة بك عن الأصل باستخدام **dch --local** *version-identifier*، أو تعديل تفاصيل الحزمة الأخرى باستخدام **dch**.

تطبيق التصحيح باستخدام **patch -p1 <** *patch-file* أو تعديل سلسلة **quilt**.

تعديل خيارات البناء، عادةً ما توجد في ملف **debian/rules** الخاص بالحزمة، أو الملفات الأخرى في المجلد **debian/**.

بعد تعديل حزمة مصدر، يمكنك بناء الحزمة الثنائية باستخدام:

```
dpkg-buildpackage -us -uc -bf
```

من مجلد المصدر، والذي سينشئ حزمة ثنائية غير موقعة. يمكن بعد ذلك تثبيت الحزمة باستخدام:

```
dpkg -i package-name_version_arch.deb.
```

٢.٥.٩. تلميحات موجزة لإعادة تجميع نواة Linux

كمستخدم متقدم، قد ترغب في إعادة ترجمة نواة Kali. قد ترغب في تقليل نواة Kali القياسية، والتي يتم تحميلها بالعديد من الميزات وبرامج التشغيل، أو إضافة برامج تشغيل أو ميزات غير قياسية، أو تطبيق تصحيحات النواة. ولكن احذر: قد تؤدي نواة تم ضبطها بشكل خاطئ إلى زعزعة استقرار نظامك ويجب أن تكون مستعدًا لقبول أن Kali لا يمكنها ضمان تحديثات الأمان لنواة مخصصة.

بالنسبة لمعظم تعديلات النواة، ستحتاج إلى تثبيت بعض الحزم بـ:

```
apt install build-essential libncurses5-dev fakeroot
```

يجب أن يسرد الأمر **apt-cache search ^linux-source** أحدث إصدار من نواة تم تعبئته بواسطة Kali، ويقوم:

```
apt install linux-source-version-number
```

بتثبيت أرشيف مضغوط لمصدر النواة في **/usr/src**.

يجب استخراج ملفات المصدر باستخدام **tar -xaf** في مجلد مختلف عن **/usr/src** (مثل **~/kernel**).

عندما يحين الوقت لتكوين نواة الخاص بك، ضع هذه النقاط في الاعتبار:

ما لم تكن مستخدمًا متقدمًا، يجب عليك أولاً تعبئة ملف تكوين النواة. الطريقة المفضلة هي استعارة التكوين القياسي لـ Kali عن طريق نسخ **/boot/config-***version-string* إلى **~/kernel/linux-source-***version-number***/.config**. بدلاً من ذلك، يمكنك استخدام **make** *architecture***_defconfig** للحصول على تكوين معقول للبنية المحددة.

ستقوم أداة تكوين نواة **make menuconfig** القائمة على النص بقراءة ملف **config.** وتقديم جميع عناصر التكوين في قائمة ضخمة يمكنك التنقل فيها. يُظهر لك تحديد عنصر توثيقه وقيمه المحتملة ويسمح لك بإدخال قيمة جديدة.

عند تشغيله من مجلد مصدر النواة الخاص بك، ستؤدي عملية التنظيف **make clean** إلى إزالة الملفات التي تم تجميعها سابقًا وستعمل **make deb-pkg** على إنشاء ما يصل إلى خمس حزم ديبان. يحتوي ملف **deb.** linux-image-version على صورة النواة والوحدات المرتبطة بها.

لاستخدام النواة المدمجة فعلياً، قم بتثبيت الحزم المطلوبة باستخدام **dpkg -i** *file.deb*. حزمة "صورة لينكس" مطلوبة؛ ما عليك سوى تثبيت حزمة "linux-headers" إذا كان لديك بعض وحدات النواة الخارجية التي يجب إنشاؤها، وهذا هو الحال إذا كان لديك بعض حزم "-*dkms" مثبتة (راجع **dpkg -l "*-dkms" | grep ^ii**). لا تحتاج الحزم الأخرى بشكل عام (إلا إذا كنت تعرف لماذا تحتاجها!).

٣.٥.٩. نصائح موجزة لبناء صور ISO مخصصة لـ Kali Live

تم إنشاء صور Kali ISO الرسمية ببناء مباشر، وهو عبارة عن مجموعة من البرامج النصية التي تتيح الأتمتة والتخصيص الكامل لجميع جوانب إنشاء صورة ISO.

يجب أن يكون نظام Kali محدثًا بالكامل قبل استخدام الإصدار المباشر.

يمكن استرداد تكوين Kali للبناء المباشر من مستودعات Gali في Git باستخدام أمرين:

```
apt install curl git live-build
```

متبوعًا بـ:

```
git clone git://gitlab.com/kalilinux/build-scripts/live-build-config.git
```

لإنشاء صورة Kali ISO محدثة ولكن غير معدلة، ما عليك سوى تشغيل -- **./build.sh verbose**. سيستغرق البناء وقتًا طويلاً حتى يكتمل حيث سيتم تنزيل جميع الحزم لتضمينها. عند الانتهاء، ستجد صورة ISO الجديدة في مجلد **images**. إذا قمت بإضافة **--variant** *variant* إلى سطر الأوامر، فسيقوم بإنشاء المتغير المحدد لصورة Kali ISO. يتم تعريف المتغيرات المختلفة من خلال أدلة التكوين الخاصة بهم **kali-config/variant-***. الصورة الرئيسية هي متغير "variant" **gnome**.

هناك عدة طرق لتخصيص ISO الخاص بك عن طريق تعديل مجلد التكوين للبناء المباشر:

يمكن إضافة الحزم إلى (أو إزالتها من) ISO المباشر عن طريق تعديل ملفات **package-lists/*.list.chroot**.

يمكن تضمين الحزم المخصصة في الصورة الحية عن طريق وضع ملفات **deb.** في مجلد **packages.chroot**. يمكن توقع التثبيت باستخدام ملفات **preseed/*.cfg**.

يمكنك إضافة ملفات إلى نظام الملفات المباشر بوضعها في موقعها المتوقع تحت مجلد التكوين **includes.chroot**.

يمكنك تنفيذ النصوص البرمجية أثناء عملية إعداد chroot للنظام المباشر عن طريق تثبيتها كملفات **hooks/live/*.chroot**. يمكنك أيضًا تنفيذ البرامج النصية في وقت الإقلاع للصورة المباشرة التي تم بناؤها: يجب عليك ترتيبها لتثبيتها في **/usr/lib/live/config/***XXXX-name*، على سبيل المثال من خلال الاعتماد على مجلد التكوين **includes.chroot**.

يعد دليل أنظمة Debian Live مرجعًا ممتازًا لتكوين واختبار النظام المباشر.

إعداد ثبات مشفر وغير مشفر على مفتاح USB: من السهل إنشاء تثبيت Kali Live USB قياسي. على الرغم من أن العملية قد تبدو معقدة من الناحية البنائية، إلا أنه من السهل نسبياً إضافة كل من الثبات المشفر وغير المشفر إلى التثبيت المحمول لتوسيع وظائفه بشكل كبير.

في الفصل التالي، سنناقش كيفية تحجيم كالي للمشروع. سنناقش إدارة التكوين ونوضح لك كيفية توسيع وتخصيص Kali Linux بطريقة سهلة النشر سواء كان لديك زوج من الأجهزة، أو عدة آلاف.

التمرين الأول لـلفصل التاسع- hook حزمة كالي

١. hook حزمة **kali-meta**.

٢. أضف ملفات حزم meta جديدة تحتوي على ٣ فقط من أدواتك المفضلة.

٣. قم بإنشاء ملفات deb الثنائية لاستخدامها لاحقًا.

الإجابة:

١. أولاً، دعنا نحدث ملف المصادر ليشمل حزم المصدر:

```
apt-get install devscripts # To install dch
nano /etc/apt/sources.list
# الغي تعليق هذا السطر: deb-src http://http.kali.org/kali kali-rolling main non-free contrib
```

بعد ذلك، احصل على المصدر. لاحظ أن أرقام نسختك قد تختلف:

```
apt-get update
apt source kali-meta # This installs all kali-linux-* packages.

cd kali-meta-2017.2.0/
ls -l
nano debian/control
```

٢. قم بتغيير ملف التحكم. تضمين الحزمة المخصصة الخاصة بك:

```
Package: kali-linux-muts
Architecture: any
Depends: ${misc:Depends},
 kali-linux,
 aircrack-ng,
 nmap,
 sqlmap,
```

```
Description: Kali Linux Custom tools for muts
 This is Kali Linux, the most advanced penetration testing and security
 auditing distribution.
 .
 This metapackage depends on few of muts' favorites.
```

قم بتغيير رقم إصدار الحزمة بحيث يمكن تمييز الحزم المعاد بناؤها عن الأصلية:

```
root@kali:~/kali-meta-2017.2.0# head -1 debian/changelog
root@kali:~/kali-meta-2017.2.0#dch --local muts -m "Added a new metapackage"
root@kali:~/kali-meta-2017.2.0# head -1 debian/changelog # Check that the changes were made
```

٣. أخيرًا، قم ببناء الحزمة:

```
root@kali:~/kali-meta-2017.2.0# dpkg-buildpackage -us -uc -b # Disable signatures (-us -uc), binary-only build (-b)
root@kali:~/kali-meta-2017.2.0# ls -l ../*muts*
-rw-r--r-- 1 root root  6804 Aug 28 13:42 gqrx_2017.2.0muts1_all.deb
-rw-r--r-- 1 root root  6948 Aug 28 13:42 kali-desktop-common_2017.2.0muts1_all.deb
-rw-r--r-- 1 root root  6972 Aug 28 13:42 kali-desktop-gnome_2017.2.0muts1_all.deb
-rw-r--r-- 1 root root  6796 Aug 28 13:42 kali-desktop-kde_2017.2.0muts1_all.deb
-rw-r--r-- 1 root root  6920 Aug 28 13:42 kali-desktop-live_2017.2.0muts1_all.deb
-rw-r--r-- 1 root root  6812 Aug 28 13:42 kali-desktop-lxde_2017.2.0muts1_all.deb
-rw-r--r-- 1 root root  6868 Aug 28 13:42 kali-desktop-xfce_2017.2.0muts1_all.deb
-rw-r--r-- 1 root root  7068 Aug 28 13:42 kali-linux_2017.2.0muts1_amd64.deb
```

```
-rw-r--r-- 1 root root  7062 Aug 28 13:42 kali-linux-all_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  7290 Aug 28 13:42 kali-linux-forensic_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  8732 Aug 28 13:42 kali-linux-full_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  6850 Aug 28 13:42 kali-linux-gpu_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  6844 Aug 28 13:42 kali-linux-muts_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  7298 Aug 28 13:42 kali-linux-nethunter_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  7088 Aug 28 13:42 kali-linux-pwtools_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  6864 Aug 28 13:42 kali-linux-rfid_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  6908 Aug 28 13:42 kali-linux-sdr_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  6924 Aug 28 13:42 kali-linux-top10_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  6942 Aug 28 13:42 kali-linux-voip_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  7360 Aug 28 13:42 kali-linux-web_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root  7058 Aug 28 13:42 kali-linux-wireless_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root 10312 Aug 28 13:42 kali-meta_2017.2.0muts1_amd64.buildinfo
-rw-r--r-- 1 root root  8343 Aug 28 13:42 kali-meta_2017.2.0muts1_amd64.changes

root@kali:~/kali-meta-2017.2.0# ls -l ../kali-linux-muts_2017.2.0muts1_amd64.deb
-rw-r--r-- 1 root root 6852 Aug 28 14:05 ../kali-linux-muts_2017.2.0muts1_amd64.deb
```

التمرين الثاني للفصل التاسع - تحديث حزمة Kali

١. حزم أحدث نسخة مطلقة من **SET** للاستخدام مع كالي.

٢. قم بإنشاء ملف deb الثنائي ليستخدم لاحقًا.

٣. هل يمكنك تحديث الحزمة **aircrack-ng** بنفس الطريقة؟

الإجابة:

١. أولاً، احصل على إصدار Kali من SET:

```
apt source set
```

بعد ذلك، احصل على أحدث إصدار من SET. لاحظ أن أرقام نسختك قد تختلف:

```
wget https://github.com/trustedsec/social-engineer-toolkit/archive/master.tar.gz -O set 7.7.1.orig.tar.gz
```

```
tar xvf set_7.7.1.orig.tar.gz
```

للتوضيح، قم بإعادة تسمية الإصدار الأخير.

```
mv social-engineer-toolkit-master social-engineer-toolkit-7.7.1
```

انسخ جميع المواد الخاصة بديبيان على:

```
cp -a set-7.7/debian social-engineer-toolkit-7.7.1/debian
rm -rf social-engineer-toolkit-7.7.1/.git
```

تحديث رقم الإصدار:

```
cd social-engineer-toolkit-7.7.1
head -1 debian/changelog
dch -v 7.7.1-0muts1 "New upstream release"
head -1 debian/changelog
```

٢. تنفيذ البناء الفعلي والتحقق من أنه يعمل:

```
dpkg-buildpackage -us -uc -b
ls -l ../*muts* # with whatever version tag you used
dpkg -i ../set_7.7.1-0muts1_all.deb # with whatever version tag you used
```

بالنسبة إلى **aircrack-ng**، نوع مماثل من التحديث:

```
nano /etc/apt/sources.list
apt-get update
apt source aircrack-ng
wget https://github.com/aircrack-ng/aircrack-ng/archive/master.tar.gz
tar zxpf master.tar.gz
mv aircrack-ng-master aircrack-ng-1.3
cp -rf aircrack-ng-1.2-0~rc4/debian/ aircrack-ng-1.3/
```

```
cd aircrack-ng-1.3/
head -1 debian/changelog
dch -v 1:1.3 -m "Upstream update"
nano debian/changelog
dpkg-checkbuilddeps
apt-get install libgcrypt-dev libgcrypt11-dev libnl-genl-3-dev libpcap0.8-dev libpcre3-dev libsqlite3-dev pkg-config zlib1g-dev
dpkg-buildpackage -us -uc –b
```

التمرين الثالث للفصل التاسع - إعادة بناء نواة خاصة بك

تم بناء نواة Kali بفلسفة "مقاس واحد يناسب الجميع"، لتكون قادرة على دعم أكبر قاعدة ممكنة من الأجهزة.

١. تثبيت أداة قياس الأداء مثل likwid وإطلاق مقياس مرجعي سريع مثل likwid-bench.

٢. قم بتثبيت "Kernel GCC patch" الخاص بـ graysky2 لتحسين نواة وحدة المعالجة المركزية الخاصة بك.

٣. أعد تجميع هذه النواة بمجرد إضافة التصحيح وتحديد نوع طراز CPU الخاص بك.

الإجابة:

١. تثبيت Likewid، إطلاق معيار:

```
apt-get install likwid

likwid-topology -g | head # to find out which processor you have

likwid-bench -t copy -w S0:100kB:1 # to run a quick benchmark on socket 0
```

٢. يمكن العثور على تصحيح تحسين معالج النواة هنا. تثبيت التبعيات المطلوبة لأداء ترجمة النواة. لاحظ أن أرقام نسختك قد تختلف:

```
apt install build-essential libncurses5-dev fakeroot
apt-cache search ^linux-source # search for the current linux-source package version
apt install linux-source-4.9 # grab it
ls /usr/src # which gets extracted to /usr/src
```

٣. استخرج مصادر النواة، وانسخ ملف التكوين الحالي.

```
mkdir ~/kernel; cd ~/kernel
tar -xaf /usr/src/linux-source-4.9.tar.xz
cp /boot/config-4.9.0-kali3-amd64 ~/kernel/linux-source-4.9/.config # Copy existing config
```

قم بتشغيل menuconfig على تكوين النواة الذي لم يتم إصلاحه:

```
cd linux-source-4.9
make menuconfig
```

انتقل إلى الموقع التالي في تهيئة النواة وتحقق من خياراتك:

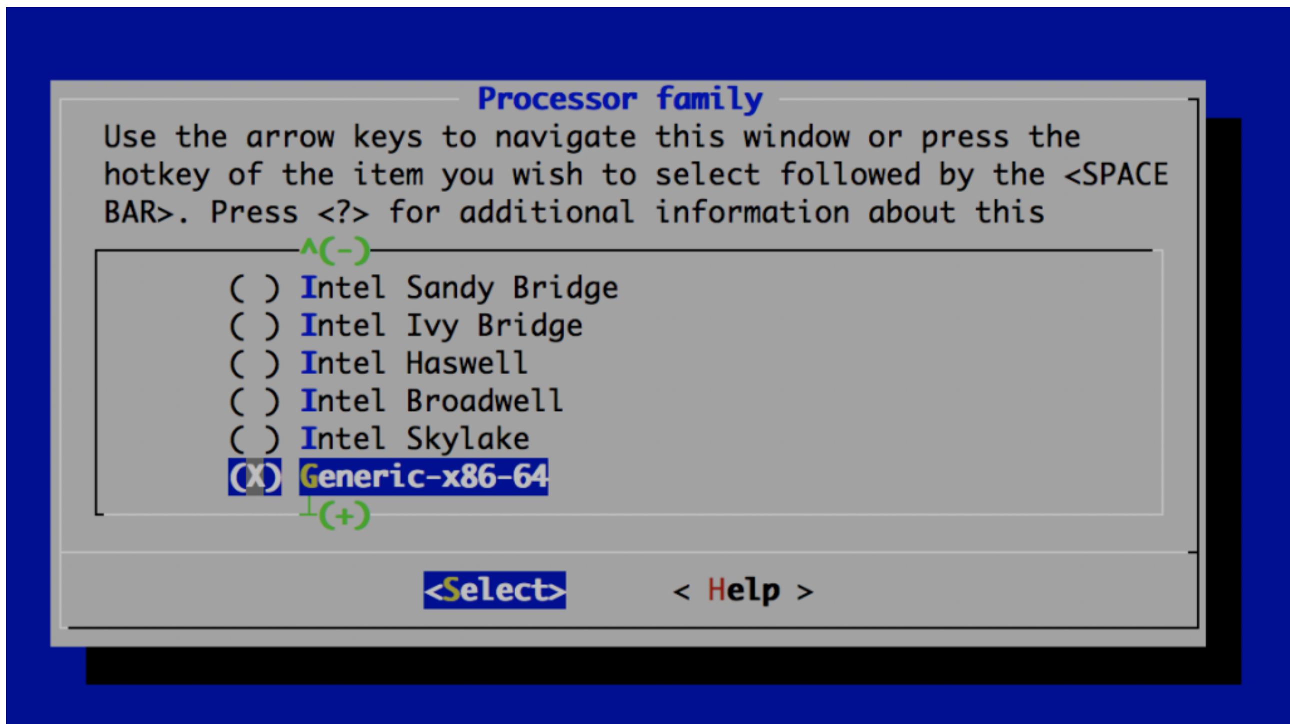
```
Processor type and features  --->
  Processor family (Generic-x86-64)  --->
```

اخرج من التكوين بدون حفظ. قم بتنزيل تصحيح التحسين، وقم بتصحيح النواة:

```
cd ~/kernel
wget
https://raw.githubusercontent.com/graysky2/kernel_gcc_patch/master/enable_additional_cpu_optimizations_for_gcc_v4.9%2B_kernel_v3.15%2B.patch
cd linux-source-4.9/
patch -p1 <
../enable_additional_cpu_optimizations_for_gcc_v4.9+_kernel_v3.15+.patch
make menuconfig
```

مرة أخرى قم بزيارة خيارات تكوين النواة لنموذج وحدة المعالجة المركزية. سترى خيارات جديدة:

```
Processor type and features --->
  Processor family (Generic-x86-64) --->
```



اختر نوع وحدة المعالجة المركزية ذات الصلة، واحفظ ثم قم بإنهاء التكوين. الآن قم ببناء نواة الخاص بك.

export CONCURRENCY_LEVEL=5 #number of CPUs you have +1

make deb-pkg LOCALVERSION=-custom KDEB_PKGVERSION=$(make kernelversion)-1

أطلق معيارًا آخر:

likwid-topology -g | **head** # to find out which processor you have

likwid-bench -t copy -w S0:100kB:1 # to run a quick benchmark on socket 0

هل تحسنت معاييرك؟ ربما يمكنك أن تتصل: /* أشعر بخيبة الأمل*/

التمرين الرابع البناء المباشر لكالي - الأداة المناسبة للمهمة الصحيحة

في هذا المشهد من Mr.robot، كان على أنجيلا تشغيل محرك أقراص USB Kali، وإدخال عدة أوامر من أجل إنجاز مهمتها. هل يمكنك بناء كالي ISO مخصص من شأنه تحسين ذلك؟ أتمتة العملية حتى لا تضطر أنجيلا إلى لمس لوحة المفاتيح بعد تشغيل كالي.

الإجابة:

قم ببناء ISO مباشر لأنجيلا. أريها كيف يتم ذلك!

```
# حدث نظامك
apt-get update
apt-get dist-upgrade

# تثبيت الأدوات المطلوبة
apt install -y git live-build cdebootstrap curl

# تنزيل الملفات المطلوبة لبناء النظام المباشر
git clone git://gitlab.com/kalilinux/build-scripts/live-build-config.git

# استبدال قوائم الحزم الافتراضية بالحد الأدنى المطلوب من الحزم
cd live-build-config/
cat kali-config/variant-default/package-lists/kali.list.chroot
echo cryptsetup > kali-config/variant-default/package-lists/kali.list.chroot
echo openssh-server >> kali-config/variant-default/package-lists/kali.list.chroot
```

```
echo nmap >> kali-config/variant-default/package-lists/kali.list.chroot

# إضافة ملفات إلى نظام الملفات المباشر (تكوين البرنامج النصي لبدء التشغيل المخصص)
mkdir -p kali-config/common/includes.chroot/lib/systemd/system/

# قم بتسجيل خدمة "أنجيلا" مخصصة لتشغيل /usr/bin/startssh
cat << EOF > kali-config/common/includes.chroot/lib/systemd/system/angela.service
[Unit]
Description=Start Custom Script
After=multi-user.target

[Service]
Type=idle
ExecStart=/bin/bash /usr/bin/startssh

[Install]
WantedBy=multi-user.target
EOF

# Create /usr/bin (and parents) on live file system
mkdir -p kali-config/common/includes.chroot/usr/bin/
```

```
# Create a "startssh" script to do our nefarious things
cat << EOF > kali-config/common/includes.chroot/usr/bin/startssh
#!/bin/sh
echo hola > /root/test.txt
EOF
# Create live hook to enable our custom service
cat << EOF > kali-config/common/hooks/live/angela.chroot
#!/bin/sh
systemctl enable angela.service || true
EOF
# اجعله قابلا للتشغيل
chmod 755 kali-config/common/hooks/live/angela.chroot
# Create boot config file, adjust prompt, timeout, autoboot, etc:
cat << EOF > kali-config/common/includes.binary/isolinux/isolinux.cfg
include menu.cfg
default vesamenu.c32
prompt 0
timeout 20
ONTIMEOUT live-amd64
EOF
# Build the ISO!
./build.sh –verbose
```

التمرين الخامس - برنامج التثبيت التلقائي المصغر التلقائي لـ Kali

قم بإنشاء ISO للتثبيت الذاتي يحتوي على الحد الأدنى من الحزم الممكنة، ويتضمن فقط opensh-server و salt-minion.

أضف مفاتيح SSH العامة الخاصة بك إلى هذه الصورة ليسهل الوصول إليها لاحقًا.

تأكد من عمل ISO كما هو متوقع. سنستخدم هذا ISO في الفصل التالي.

الإجابة:

يستخدم البناء المباشر بنية مجلد كامل كمدخل لتكوينه. نقوم بتخزين هذا التكوين وبعض البرامج النصية المساعدة المرتبطة في مستودع Git للبناء المباشر. سنستخدم هذا المستودع كأساس لبناء صور مخصصة. قم بتثبيت الحزم المطلوبة وتنزيل مستودع Git مع تكوين Kali للبناء المباشر:

```
apt install curl git live-build
```

```
git clone git://gitlab.com/kalilinux/build-scripts/live-build-config.git
```

```
cd live-build-config
```

قم بإنشاء قائمة الحزم لتضمينها، بدءًا من salt-minion:

```
echo salt-minion > kali-config/variant-default/package-lists/kali.list.chroot
```

.. أضف أخرى.

```
echo openssh-server >> kali-config/variant-default/package-lists/kali.list.chroot
```

قم بإنشاء دليل للتضمين، وقم بوضع ملف الضغط المخصص لدينا pressed.cfg.

```
mkdir -p kali-config/common/includes.installer
wget https://www.kali.org/dojo/preseed.cfg -O ./kali-config/common/includes.installer/preseed.cfg
```

يمكنك إضافة ملفات إلى صورة ISO بوضعها في موقعها المتوقع تحت مجلد config.binary. على سبيل المثال، install.cfg (خيارات قائمة الإقلاع) ...

```
cat << EOF > kali-config/common/includes.binary/isolinux/install.cfg
label install
menu label ^Install
linux /install/vmlinuz
initrd /install/initrd.gz
append vga=788 --quiet file=/preseed.cfg locale=en_US keymap=us hostname=kali domain=local.lan
EOF
```

.. وملف isolinux.cfg مع خيارات الإقلاع:

```
cat << EOF > kali-config/common/includes.binary/isolinux/isolinux.cfg
include menu.cfg
ui vesamenu.c32
default install
prompt 0
timeout 5
EOF
echo 'systemctl enable ssh' > kali-config/common/hooks/live/01-start-ssh.chroot
```

أضف مفتاح SSH إلى ISO:

```
ssh-keygen -f /root/.ssh/id_rsa -t rsa -N '' # اختياري إذا كنت قد فعلت ذلك بالفعل!

mkdir -p kali-config/common/includes.chroot/root/.ssh/
cat /root/.ssh/id_rsa.pub > kali-config/common/includes.chroot/root/.ssh/authorized_keys
```

بناء الصورة:

```
./build.sh --verbose
```

التمرين السادس للفصل التاسع - Live USB متعدد المخازن الثابتة و LUKS Nuke

قم بإنشاء USB مباشر متعدد المخازن الثابتة وتمكين كلمة مرور LUKS Nuke.

الإجابة:

في هذا القسم، نفترض أنك أعددت مفتاح Kali Live USB باتباع الإرشادات الواردة في القسم ٤.١.٢، "نسخ الصورة على قرص DVD أو مفتاح USB" وأنك استخدمت مفتاح USB كبيراً بما يكفي لاستيعاب صورة ISO (حوالي ٣ غيغابايت) وبيانات الدلائل التي تريد استمرارها. نفترض أيضًا أن نظام USB يتم التعرف عليه من خلال Linux كـ dev/sdb/ وأنه يحتوي فقط على القسمين اللذين يمثلان جزءًا من صورة ISO الافتراضية (dev/sdb1/ و dev/sdb2/). كن حذرا للغاية عند تنفيذ هذا الإجراء. يمكنك بسهولة تدمير البيانات المهمة إذا قمت بإعادة تقسيم محرك الأقراص الخاطئ.

قم بتوصيل جهاز USB الخاص بك في VM (أو الحاسوب) وحدد اسم الجهاز باستخدام **dmesg** أو **fdisk**. سنفترض أن اسمه dev/sdb/. قم بفصل أي أقسام إذا كانت تعمل تلقائيًا. ابدأ عملية التقسيم.

```
umount /dev/sdb1
umount /dev/sdb2
parted /dev/sdb
```

لهذا العرض التوضيحي، سنقوم بإنشاء متجرين دائمين - حيث يتم تشفير أحدهما والآخر لا.

```
(parted) print
Model: SanDisk Ultra USB 3.0 (scsi)
Disk /dev/sdb: 124GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system  Flags
1       32.8kB  2794MB  2794MB  primary               boot, hidden
2       2794MB  2794MB  721kB   primary

(parted) mkpart primary 2794 5000
(parted) mkpart primary 5000 100%
(parted) quit
Information: You may need to update /etc/fstab.
```

يقوم الأمر **mkpart** الابتدائي ٢٧٩٤ ٥٠٠٠، بعمل أول قسم جديد (القسم الثالث في المجموع)، والذي سيبدأ عند ٢٧٩٤ ميجا بايت، وينتهي عند ٥٠٠٠ ميجا بايت. نحن نستخدم قيمة البدء هذه، لأن صورة Kali الخاصة بنا تستهلك فقط ٢٧٩٤ ميجابايت على الجهاز. قد تضطر إلى تغيير هذه القيم اعتمادًا على حجم صورة Kali وجهاز USB.

بمجرد إنشاء القسمين الجديدين، يمكننا الآن البدء في تكوينهم كأقسام ثابتة في بيئة إقلاع Kali Linux. نبدأ باستخدام sdb3 لمخزننا الغير مشفر. نقوم أولاً بتهيئة القسم، ثم نعطيه استمرارية تسمية. هذا التصنيف مهم. إذا تخطيت هذا، أو أخطأت في تهجئته، فلن ينجح الثبات!

```
mkfs.ext3 /dev/sdb3
e2label /dev/sdb3 persistence
```

بعد ذلك، نقوم بإنشاء ملفات persistent.conf التي تحدد المجلدات التي نريد استمرارها - في هذه الحالة، نريد الثبات على جميع أنظمة الملفات:

```
mkdir -p /mnt/usb
mount /dev/sdb3 /mnt/usb
echo "/ union" > /mnt/usb/persistence.conf
umount /mnt/usb
```

بعد ذلك، نقوم بتكوين مخزن الاستمرار المشفر، وتشفير القسم باستخدام **cryptsetup**، وتهيئة القسم وتسميته، والتحقق من الإخراج، ثم تحديد ملف persistent.conf كما كان من قبل:

```
cryptsetup --verbose --verify-passphrase luksFormat /dev/sdb4
cryptsetup luksOpen /dev/sdb4 my_usb
mkfs.ext3 /dev/mapper/my_usb
e2label /dev/mapper/my_usb persistence
ls -l /dev/disk/by-label
mkdir -p /mnt/my_usb
mount /dev/mapper/my_usb /mnt/my_usb
echo "/ union" > /mnt/my_usb/persistence.conf
umount /dev/mapper/my_usb
cryptsetup luksClose /dev/mapper/my_usb
```

هذا هو! الآن يمكننا تشغيل USB، واختيار تشغيله بشكل نظيف (بدون مخزن ثابت)، مع مخزن ثابت غير المشفر، أو مع مخزن مشفر:

لإضافة ميزة "التدمير الذاتي" (LUKS Nuke) إلى المخزن الثابت المشفر، نحتاج ببساطة إلى تشغيل الأمر التالي:

```
cryptsetup luksAddNuke /dev/sdb4
```

اختبار الشهادة للفصل التاسع

١. أي من الأوامر التالية سينزل مصدر حزمة ديبان؟

- o dpkg –source
- o apt-get -S
- o apt source
- o aptitiude –source

٢. أي أمر سيقوم بتنزيل المصادر من مستودع GIT؟

- o git-clone
- o git-get
- o git clone
- o apt-get –git

٣. بافتراض أنك في مجلد يحتوي على حزمة مصدر غير معبأة، ما هو الأمر الذي سيقوم بتثبيت تبعيات البناء المدرجة في حقل Build-Depends في ملف debian/control؟

- o dch –build-dep
- o dpkg –build_dep
- o apt build-dep ./
- o dpkg-buildpackage

٤. ما الملف أو الأمر الذي سيكشف ما إذا كانت تغييراتك في حزمة دبيان "عالقة "stuck"" أم لا؟

- o dch –local
- o DEBCHANGES
- o debian/changelog
- o dch –updates

٥. عند تطبيق التغييرات، ما هو الأمر الذي سيقوم بتحديث البادئة المستخدمة في حزمة دبيان إلى "kali"؟

- o dch –local kali
- o dpkg-buildpackage -u kali
- o dch –prefix kali
- o dpkg-update -p kali

٦. ما هو الأمر المناسب لنسخ ملف التكوين من نسخة Kali Linux قيد التشغيل إلى شجرة مصدر Kali التي تم تنزيلها في المجلد الحالي؟

$ cp /boot/kali-linux-4.9.0-kali1-amd64/.config ~/kernel/linux-source-4.9/

$ cp /boot/kali-linux-4.9.0-kali1-amd64/.config ~/kernel/linux-source-4.9/.config

$ cp /boot/kali-linux-4.9.0-kali1-amd64/ ~/kernel/linux-source-4.9/

$ cp /boot/config-4.9.0-kali1-amd64 ~/kernel/linux-source-4.9/.config

١٠. أي أمر سينفذ أداة تكوين النواة الرسومية؟

- make config
- make gconfig
- make menuconfig
- make textconfig

١١. ما هو الأمر الذي سيقوم بتثبيت المتطلبات الأساسية لبيئة بناء Kali Linux؟

- apt install livebuild
- apt install git livebuild
- apt install curl git livebuild
- apt install curl git live-build

١٢. ما هي metapackage التي تثبت جميع الأدوات في تثبيت Kali Linux الافتراضي؟

- kali-linux
- kali-linux-all
- kali-linux-full
- kali-linux-default

١٣. أي ملف يحتوي على بيانات المجلدات الثابتة؟

- /union/persistence.conf
- **persistence.conf**
- Persistence
- persist.conf

الإجابات الصحيحة:

1. apt source
2. git clone
3. apt build-dep ./
4. **debian/changelog**
5. dch –local kali
6. $ cp /boot/config-4.9.0-kali1-amd64 ~/kernel/linux-source-4.9/.config
7. make menuconfig
8. apt install curl git live-build
9. **kali-linux-full**
10. **persistence.conf**
11. mkfs.ext3 -L persistence /dev/sdc3
12. # cryptsetup luksOpen /dev/sdb3 kali_persistence
13. # cryptsetup luksAddNuke /dev/sdb4

الفصل العاشر

كالي لينكس في المؤسسات

حتى الآن، رأينا أن Kali من مشتقات ديبان القادرة والآمنة للغاية التي توفر ميزات الأمان والتشفير ذات القوة الصناعية، وإدارة الحزم المتقدمة، والقدرات متعددة المنصات، و (ما تشتهر به) ترسانة من الطراز العالمي أدوات لأخصائي الأمن. ما قد لا يكون واضحًا هو كيف يتقدم Kali خارج نطاق سطح المكتب إلى عمليات النشر على نطاق متوسط أو كبير وحتى إلى مستوى المؤسسة. في هذا الفصل، سنوضح لك مدى قدرة Kali على التوسع خارج سطح المكتب، مما يوفر إدارة مركزية وتحكمًا على مستوى المؤسسة في العديد من عمليات تثبيت Kali Linux. باختصار، بعد قراءة هذا الفصل، ستتمكن من نشر أنظمة Kali عالية الأمان التي تم تكوينها مسبقًا لتلبية احتياجاتك الخاصة والاحتفاظ بها متزامنة بفضل تثبيت Kali (شبه التلقائي) لتحديثات الحزمة.

يتطلب هذا المستوى من المقياس عدة خطوات، بما في ذلك بدء إقلاع شبكة PXE، واستخدام أداة إدارة تكوين متقدمة (SaltStack)، والقدرة على التفرع وتخصيص الحزم، ونشر مستودع الحزم. سنقوم بتغطية كل خطوة بالتفصيل، ونوضح لك كيفية التخلص من "الرفع الثقيل"، ونشر وإدارة وصيانة العديد من عمليات تثبيت Kali Linux المخصصة بسهولة نسبية. كما لو أن ذلك لم يكن كافيًا، سنقوم بحشد من التوابع لمساعدتك في إدارة إمبراطوريتك.

١.١.١٠. تثبيت Kali Linux عبر الشبكة (PXE Boot)

كما رأينا في الفصول السابقة، فإن عملية تثبيت Kali Linux الأساسية تكون مباشرة بمجرد معرفة طريقك. ولكن إذا كان عليك تثبيت Kali على أجهزة متعددة، فقد يكون الإعداد القياسي مملاً للغاية. لحسن الحظ، يمكنك البدء في إجراء تثبيت Kali عن طريق إقلاع جهاز حاسوب عبر الشبكة. هذا يسمح لك بتثبيت كالي بسرعة وسهولة على العديد من الأجهزة في وقت واحد.

أولاً، ستحتاج إلى تشغيل الجهاز المستهدف من الشبكة. يتم تسهيل ذلك من خلال Preboot eXecution Environment (PXE)، وهي واجهة عميل/خادم مصممة لإقلاع أي جهاز متصل بالشبكة من الشبكة حتى إذا لم يكن به نظام تشغيل مثبت. يتطلب إعداد إقلاع شبكة PXE أن تقوم على الأقل بتكوين خادم بروتوكول نقل الملفات البسيط (TFTP) وخادم DHCP/BOOTP. ستحتاج أيضًا إلى خادم ويب إذا كنت ترغب في استضافة ملف Debconf سيتم استخدامه تلقائيًا في عملية التثبيت.

لحسن الحظ، يتعامل *dnsmasq* مع كل من DHCP و TFTP بحيث يمكنك الاعتماد على خدمة واحدة لإعداد كل ما تحتاجه. ويتم تثبيت خادم الويب Apache (ولكن غير ممكّن) افتراضيًا على أنظمة Kali.

خدمات DHCP و TFTP منفصلة

للحصول على إعدادات أكثر تعقيدًا، قد تكون مجموعة ميزات dnsmasq محدودة جدًا أو قد ترغب في تمكين إقلاع PXE على شبكتك الرئيسية التي تقوم بالفعل بتشغيل برنامج DHCP. في كلتا الحالتين، سيتعين عليك بعد ذلك تكوين DHCP منفصلة و DHTP منفصلة.

يغطي دليل تثبيت ديبان إعداد خادم isc-dhcp-server و tftpd-hpa لإقلاع PXE.

https://www.debian.org/releases/stable/amd64/ch04s05.html

لإعداد dnsmasq، يجب عليك أولاً تهيئتها من خلال /etc/dnsmasq.conf. يتكون التكوين الأساسي من بضعة خطوط رئيسية فقط:

```
# واجهة الشبكة المتعامل معها

interface=eth0

#خيارات DHCP

#نطاق IP للتخصيص


dhcp-range=192.168.101.100,192.168.101.200,12h
```

بوابة للإعلان للعملاء

```
dhcp-option=option:router,192.168.101.1
```

خوادم DNS للإعلان للعملاء

```
dhcp-option=option:dns-server,8.8.8.8,8.8.4.4
```

ملف الإقلاع للإعلان للعملاء

```
dhcp-boot=pxelinux.0
```

#خيارات TFTP

```
enable-tftp
```

#دليل استضافة الملفات لتقديمها

```
tftp-root=/tftpboot/
```

مع تكوين /etc/dnsmasq.conf، ستحتاج إلى وضع ملفات إقلاع التثبيت في المجلد /tftpboot/. يوفر Kali Linux أرشيف ملفات مخصصًا لهذا الغرض يمكن فكه مباشرة في /tftpboot/. ما عليك سوى الاختيار بين 32bit (i386) و 64bit (amd64) وطرق التثبيت القياسية أو الرسومية (gtk) لجهازك المستهدف واختيار الأرشيف المناسب:

http://http.kali.org/dists/kali-rolling/main/installer
amd64/current/images/netboot/gtk/netboot.tar.gz

http://http.kali.org/dists/kali-rolling/main/installer-
amd64/current/images/netboot/netboot.tar.gz

http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images/netboot/gtk/netboot.tar.gz

http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images/netboot/netboot.tar.gz

بمجرد تحديد الأرشيف، قم بإنشاء tftpboot/، قم بتنزيل الأرشيف، وفكه في هذا المجلد:

```
# mkdir /tftpboot
# cd /tftpboot
# wget http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images/netboot/netboot.tar.gz
# tar xf netboot.tar.gz
# ls -l
```

total 25896

drwxrwxr-x 3 root root 4096 May 6 04:43 debian-installer

lrwxrwxrwx 1 root root 47 May 6 04:43 ldlinux.c32 -> debian-installer/amd64/boot-screens/ldlinux.c32

-rw-r--r-- 1 root root 26507247 May 6 04:43 netboot.tar.gz

lrwxrwxrwx 1 root root 33 May 6 04:43 pxelinux.0 -> debian-installer/amd64/pxelinux.0

lrwxrwxrwx 1 root root 35 May 6 04:43 pxelinux.cfg -> debian-installer/amd64/pxelinux.cfg

-rw-rw-r-- 1 root root 71 May 6 04:43 version.info

تتضمن الملفات التي تم فك حزمتها أداة تحميل pxelinux، والتي تستخدم نفس ملفات التكوين مثل syslinux و implinux. وبسبب هذا، يمكنك تعديل ملفات الإقلاع في debian-installer/amd64/boot-screens كما تفعل عند إنشاء صور مخصصة لـ Kali Linux Live ISO.

على سبيل المثال، على افتراض أنك اخترت المثبت النصي، يمكنك إضافة معلمات الإقلاع إلى قيم اللغة والبلد وخريطة المفاتيح واسم المضيف واسم المجال. يمكنك أيضًا توجيه المثبت إلى عنوان URL خارجي وتكوين المهلة بحيث يحدث الإقلاع تلقائيًا إذا لم يتم الضغط على أي مفتاح في غضون ٥ ثوانٍ. لتحقيق ذلك، عليك أولاً تعديل ملف debian-installer/amd64/txt.cfg:

```
label install
        menu label ^Install
        kernel debian-installer/amd64/linux
        append vga=788 initrd=debian-installer/amd64/initrd.gz --- quiet language=en country=US keymap=us hostname=kali domain= url=http://192.168.101.1/preseed.cfg
```

بعد ذلك، يمكنك تعديل ملف debian-installer/amd64/syslinux.cfg لضبط المهلة:

```
# D-I config version 2.0
```

```
# search path for the c32 support libraries (libcom32, libutil etc.)
path debian-installer/amd64/boot-screens/
include debian-installer/amd64/boot-screens/menu.cfg
default debian-installer/amd64/boot-screens/vesamenu.c32
prompt 0
timeout 50
```

مسلحًا بالقدرة على تشغيل أي جهاز من الشبكة عبر PXE، يمكنك الاستفادة من جميع الميزات الموضحة في القسم ٣.٤، "التثبيتات غير المراقبة"، مما يتيح لك القيام بالإقلاع الكامل والتثبيت والتثبيت غير المراقب على أجهزة حاسوب متعددة بدون إقلاع فعلي وسائل الإعلام. أيضًا، لا تنس مرونة معلمة الإقلاع **preseed/url=http://*server*/preseed.cfg** (ولا استخدام الاسم المستعار لعنوان url)، والذي يسمح لك بتعيين ملف متنبأ يستند إلى الشبكة.

٢.١٠. الاستفادة من إدارة التكوين

مع القدرة على تثبيت Kali على أجهزة حاسوب متعددة بسرعة كبيرة، ستحتاج إلى بعض المساعدة في إدارة هذه الأجهزة بعد التثبيت. يمكنك الاستفادة من أدوات إدارة التكوين لإدارة الأجهزة أو تكوين أجهزة الحاسوب البديلة لأي حالة مرغوبة.

يحتوي Kali Linux على العديد من أدوات إدارة التكوين الشائعة التي قد ترغب في استخدامها (ansible، chef، puppet، saltstack ، إلخ) ولكن في هذا القسم، سنغطي فقط SaltStack.

https://saltstack.com

١.٢.١٠. إعداد SaltStack

SaltStack هي خدمة إدارة تكوين مركزية: *salt master* يدير العديد من *salt minions*. يجب عليك تثبيت حزمة *salt-master* على خادم يمكن الوصول إليه من قبل جميع المضيفين الذين تريد إدارتهم وsalt-minion على المضيفين الذين ترغب في إدارتهم. يجب إخبار كل عميل بمكان العثور على master الخاص به. ببساطة قم بتحرير /etc/salt/minion وقم بتعيين المفتاح الرئيسي "**master**" لاسم DNS (أو عنوان IP) الخاص بـSalt master. لاحظ أن Salt يستخدم YAML كتنسيق للملفات التكوين الخاصة به.

```
minion# vim /etc/salt/minion
minion# grep ^master /etc/salt/minion
master: 192.168.122.105
```

لكل عميل "minion" معرف فريد مخزن في etc/salt/minion_id/، والذي يتم تعيينه افتراضياً على اسم المضيف الخاص به. سيتم استخدام معرف العميل هذا في قواعد التكوين وعلى هذا النحو، من المهم تعيينه بشكل صحيح قبل أن يفتح العميل اتصاله بالسيد:

```
minion# echo kali-scratch >/etc/salt/minion_id
minion# systemctl enable salt-minion
minion# systemctl start salt-minion
```

عند تشغيل خدمة *salt-minion*، ستحاول الاتصال master Salt لتبادل بعض مفاتيح التشفير. على من جانب الـ master، يجب عليك قبول المفتاح الذي يستخدمه العميل لتعريف نفسه للسماح بالاتصال. ستكون الاتصالات اللاحقة تلقائية:

```
master# systemctl enable salt-master
master# systemctl start salt-master
master# salt-key --list all
```

Accepted Keys:

Denied Keys:

Unaccepted Keys:

kali-scratch

Rejected Keys:

```
master# salt-key --accept kali-scratch
```

The following keys are going to be accepted:

Unaccepted Keys:

kali-scratch

Proceed? [n/Y] y

Key for minion kali-scratch accepted.

٢.٢.١٠. تنفيذ الأوامر على العملاء "Minions"

بمجرد أن يتم توصيل العملاء، يمكنك تنفيذ الأوامر عليهم من السيد "master":

master# salt '*' test.ping

kali-scratch:

True

kali-master:

True

يطلب هذا الأمر من كل العملاء ('*' هو حرف بدل يستهدف كل العملاء) لتنفيذ وظيفة **ping** من وحدة تنفيذ الاختبار "**test**". تقوم هذه الوظيفة بإرجاع قيمة **True** عند النجاح وهي طريقة بسيطة للتأكد من أن الاتصال يعمل بين الرئيس والعملاء.

يمكنك أيضًا استهداف عميل معين عن طريق إعطاء معرفه في المعلمة الأولى، أو ربما مجموعة فرعية من التوابع باستخدام حرف بدل أقل عامة (مثل 'kali-*' أو '*-scratch'). فيما يلي مثال على كيفية تنفيذ أمر shell تعسفي على عملاء kali-scratch:

```
master# salt kali-scratch cmd.shell 'uptime; uname -a'
```

kali-scratch:

05:25:48 up 44 min, 2 users, load average: 0.00, 0.01, 0.05

Linux kali-scratch 4.5.0-kali1-amd64 #1 SMP Debian 4.5.3-2kali1 (2016-05-09) x86_64 GNU/Linux

مرجع وحدة salt

هناك العديد من وحدات التنفيذ المتاحة لجميع أنواع حالات الاستخدام. لن نغطيها جميعًا هنا، ولكن القائمة الكاملة متاحة في https://docs.saltstack.com/en/latest/ref/modules/all/index.html. يمكنك أيضًا الحصول على وصف لجميع وحدات التنفيذ ووظائفها المتاحة في أحد العملاء المعينين باستخدام الأمر **salt** *minion* **sys.doc**. يؤدي تشغيل هذا الأمر إلى إرجاع قائمة طويلة جدًا من الوظائف، ولكن يمكنك تصفية القائمة بتمرير اسم وظيفة أو وحدة مسبوقة ببادئة من قبل الوحدة الرئيسية كمعلمة:

master# salt kali-scratch sys.doc disk.usage

disk.usage:

Return usage information for volumes mounted on this minion

واحدة من أكثر الوحدات المفيدة هي pkg، وهي عبارة عن تجريد مدير الحزم بالاعتماد على مدير الحزم المناسب للنظام (apt-get لديبيان ومشتقاته مثل Kali). يقوم الأمر pkg.refresh_db بتحديث قائمة الحزم (أي أنه يقوم بـ apt-get update) بينما يقوم pkg.upgrade بتثبيت جميع التحديثات المتاحة (يقوم بـ apt-get upgrade أو apt-get dist-upgrade، اعتماداً على الخيارات المستلمة). يسرد الأمر pkg.list_upgrades عمليات الترقية المعلقة (التي سيتم تنفيذها بواسطة الأمر pkg.upgrade dist_upgrade=True).

وحدة **service** عبارة عن تجريد لمدير الخدمة (systemd في حالة Kali)، والذي يتيح لك تنفيذ جميع عمليات systemctl المعتادة: service.enable، service.disable، service.start، service.stop، service.restart، و service.reload:

```
master# salt '*' service.enable ssh
kali-scratch:
    True
kali-master:
    True
master# salt '*' service.start ssh
kali-master:
    True
```

```
kali-scratch:
    True
master# salt '*' pkg.refresh_db
kali-scratch:
    ----------
kali-master:
    ----------
master# salt '*' pkg.upgrade dist_upgrade=True
kali-scratch:
    ----------
    changes:
        ----------
        base-files:
            ----------
            new:
                1:2016.2.1
            old:
                1:2016.2.0
[...]
```

```
        zaproxy:
            ----------
            new:
                2.5.0-0kali1
            old:
                2.4.3-0kali3
    comment:
    result:
        True
```

كعينة أكثر واقعية، يمكنك بسهولة إعداد مسح Nmap باستخدام dnmap. بعد تثبيت الحزمة على كل العملاء، تبدأ الخادم في المحطة الأولى:

```
server# salt '*' pkg.install dnmap
[...]
server# vim dnmap.txt
server# dnmap_server -f dnmap.txt
```

باقتراض أن عنوان IP للخادم هو ٤.٣.٢.١، يمكنك بعد ذلك إخبار جميع العملاء لبدء عملية العميل التي تتصل بالخادم:

```
server# salt '*' cmd.run_bg template=jinja
'dnmap_client -s 1.2.3.4 -a {{ grains.id }}'
```

kali-scratch:

```
    ----------
    pid:
        17137
[...]
```

لاحظ أن المثال يستخدم **cmd.run_bg** لتشغيل الأمر **dnmap_client** في الخلفية. لا تنتظر حتى تنتهي، لأنها عملية طويلة الأمد. لسوء الحظ، فإنه لا يقتل نفسه بشكل صحيح عند مقاطعة الخادم لذلك قد تضطر إلى تنظيفه:

```
server# salt '*' cmd.shell 'pkill -f dnmap_client'
```

٣.٢.١. حالات salt والميزات الأخرى

على الرغم من أن التنفيذ عن بُعد هو لبنة بناء مهمة، إلا أنه جزء صغير جدًا مما يمكن أن يفعله SaltStack.

عند إعداد جهاز جديد، غالبًا ما تقوم بتشغيل العديد من الأوامر والاختبارات لتحديد تفاصيل النظام قبل التثبيت. يمكن إضفاء الطابع الرسمي على هذه العمليات في قوالب تكوين قابلة لإعادة الاستخدام تسمى *state files*. يمكن بعد ذلك تنفيذ العمليات الموضحة في ملفات الحالة باستخدام أمر salt وهو **`state.apply`**.

لتوفير بعض الوقت، يمكنك الاعتماد على العديد من ملفات الحالة الجاهزة للاستخدام التي تم إنشاؤها من قبل المجتمع والتي يتم توزيعها في "Salt formulas":

https://docs.saltstack.com/en/latest/topics/development/conventions/formulas.html

هناك العديد من الميزات الأخرى التي يمكن دمجها:

Scheduled execution of actions

Defining actions in response to events triggered by minions

Collecting data out of minions

Orchestration of a sequence of operations across multiple minions

Applying states over SSH without installing the salt-minion service

Provisioning systems on cloud infrastructures and bringing them under management

And more

SaltStack واسع جدًا ولا يمكننا تغطية جميع الميزات هنا. في الواقع، هناك كتب مخصصة بالكامل لـ SaltStack والوثائق عبر الإنترنت واسعة جدًا أيضًا. تحقق منه إذا كنت تريد معرفة المزيد عن ميزاته:

https://docs.saltstack.com/en/latest/

إذا كنت تدير عددًا كبيرًا من الأجهزة، فمن المستحسن معرفة المزيد عن SaltStack حيث يمكنك توفير قدر كبير من الوقت عند نشر أجهزة جديدة وستتمكن من الحفاظ على تكوين متماسك عبر شبكتك.

لإعطائك لمحة عن كيفية العمل مع ملفات الحالة، سنغطي مثالًا بسيطًا: كيفية تمكين مستودع APT وتثبيت حزمة تقوم بإنشائها في القسم ١٠.٣.٣، "إنشاء مستودع حزمة لـ APT" والقسم ١٠.٣.٢، "إنشاء حزم التكوين". ستقوم أيضًا بتسجيل مفتاح SSH في حساب الجذر حتى تتمكن من تسجيل الدخول عن بُعد في حالة حدوث مشاكل.

بشكل افتراضي، يتم تخزين ملفات الحالة في /srv/salt على الـmaster؛ هي ملفات منظمة YAML ذات امتداد **sls.**. تمامًا مثل تشغيل الأوامر، يعتمد تطبيق الحالة على العديد من وحدات الحالة:

https://docs.saltstack.com/en/latest/topics/tutorials/starting_states.html

https://docs.saltstack.com/en/latest/ref/states/all/

سيقوم ملف /srv/salt/offsec.sls باستدعاء ثلاث من هذه الوحدات:

```
offsec_repository:
  pkgrepo.managed:
    - name: deb http://pkgrepo.offsec.com offsec-internal main
    - file: /etc/apt/sources.list.d/offsec.list
    - key_url: salt://offsec-apt-key.asc
    - require_in:
      - pkg: offsec-defaults

offsec-defaults:
  pkg.installed
```

```
ssh_key_for_root:
  ssh_auth.present:
    - user: root
    - name: ssh-rsa AAAAB3NzaC1yc2...89C4N rhertzog@kali
```

تعتمد حالة **offsec_repository** على وحدة حالة **pkgrepo**. يستخدم المثال الوظيفة **managed** في تلك الوحدة النمطية لتسجيل مستودع الحزمة. باستخدام السمة **key_url**، يمكنك إخبار salt أن مفتاح GPG (ASCII) المطلوب للتحقق من توقيع المستودع يمكن جلبه من **/srv/salt/offsec-apt-key.asc** على الصفحة الرئيسية للملح "salt master". تضمن الخاصية **require_in** معالجة هذه الحالة قبل **offsec-defaults**، لأن الأخيرة تحتاج إلى تكوين المستودع بشكل صحيح لتتمكن من تثبيت الحزمة.

تقوم حالة offsec-defaults بتثبيت الحزمة التي تحمل نفس الاسم. يوضح هذا أن اسم المفتاح غالبًا ما يكون قيمة مهمة للحالات، على الرغم من أنه يمكن تجاوزه دائمًا بخاصية **name** (كما هو الحال بالنسبة للحالة السابقة). بالنسبة للحالات البسيطة مثل هذه الحالة، يمكن قراءتها وموجزة.

تضيف الحالة الأخيرة (**ssh_key_for_root**) مفتاح SSH المعطى في خاصية name إلى **/root/.ssh/authorized_keys** (يتم تعيين المستخدم الهدف في خاصية **user**). لاحظ أننا قمنا بتقصير مفتاح سهولة القراءة هنا، ولكن يجب عليك وضع المفتاح الكامل في خاصية name.

يمكن بعد ذلك تطبيق ملف الحالة هذا على أحد العملاء المعينين:

```
server# salt kali-scratch state.apply offsec
kali-scratch:
----------
          ID: offsec_repository
    Function: pkgrepo.managed
        Name: deb http://pkgrepo.offsec.com offsec-internal main
      Result: True
     Comment: Configured package repo 'deb http://pkgrepo.offsec.com offsec-internal main'
     Started: 06:00:15.767794
    Duration: 4707.35 ms
     Changes:
              ----------
              repo:
                  deb http://pkgrepo.offsec.com offsec-internal main
              ----------
          ID: offsec-defaults
    Function: pkg.installed
      Result: True
     Comment: The following packages were installed/updated: offsec-defaults
     Started: 06:00:21.325184
    Duration: 19246.041 ms
     Changes:
```

```
          ----------
          offsec-defaults:
              ----------
              new:
                  1.0
              old:
----------
          ID: ssh_key_for_root
    Function: ssh_auth.present
        Name: ssh-rsa AAAAB3NzaC1yc2...89C4N rhertzog@kali
      Result: True
     Comment: The authorized host key AAAAB3NzaC1yc2...89C4N for user root was added
     Started: 06:00:40.582539
    Duration: 62.103 ms
     Changes:
              ----------
              AAAAB3NzaC1yc2...89C4N:
                  New

Summary for kali-scratch
------------
Succeeded: 3 (changed=3)
Failed:    0
```

```
------------
Total states run:     3
Total run time:  24.015 s
```

يمكن أيضًا ربطه بشكل دائم بالعميل بتسجيله في ملف **/srv/salt/top.sls**، والذي يستخدمه الأمر `state.highstate` لتطبيق جميع الحالات ذات الصلة في مسار واحد:

```
server# cat /srv/salt/top.sls
base:
  kali-scratch:
    - offsec
server# salt kali-scratch state.highstate
kali-scratch:
----------
          ID: offsec_repository
    Function: pkgrepo.managed
        Name: deb http://pkgrepo.offsec.com offsec-internal main
      Result: True
     Comment: Package repo 'deb http://pkgrepo.offsec.com offsec-internal main' already configured
     Started: 06:06:20.650053
    Duration: 62.805 ms
     Changes:
----------
```

```
          ID: offsec-defaults
    Function: pkg.installed
      Result: True
     Comment: Package offsec-defaults is already installed
     Started: 06:06:21.436193
    Duration: 385.092 ms
     Changes:
----------
          ID: ssh_key_for_root
    Function: ssh_auth.present
        Name: ssh-rsa AAAAB3NzaC1yc2...89C4N rhertzog@kali
      Result: True
     Comment: The authorized host key AAAAB3NzaC1yc2...89C4N is already present for user root
     Started: 06:06:21.821811
    Duration: 1.936 ms
     Changes:
Summary for kali-scratch
------------
Succeeded: 3
Failed:    0
------------
Total states run:     3
Total run time: 449.833 ms
```

٣.١٠. توسيع وتخصيص كالي لينكس

في بعض الأحيان تحتاج إلى تعديل Kali Linux لتناسب احتياجاتك الخاصة. أفضل طريقة لتحقيق ذلك هي الحفاظ على مستودع الحزمة الخاص بك الذي يستضيف الإصدارات المعدلة من حزم Kali، بالإضافة إلى الحزم الإضافية التي توفر تكوينًا مخصصًا وبرامج إضافية (لا توفرها Kali Linux).

١.٣.١٠. تعديل حزم كالي

يرجى الرجوع إلى القسم ١.٩، "تعديل حزم كالي" للحصول على توضيحات حول هذا الموضوع.

يمكن أن تكون جميع الحزم متشعبة إذا كان لديك سبب وجيه ولكن يجب أن تدرك أن طلب الحزمة له تكلفة، حيث يجب عليك تحديثه في كل مرة تنشر Kali تحديثًا. إليك بعض الأسباب التي قد تدفعك إلى تعديل حزمة:

- ❖ لإضافة تصحيح لإصلاح خطأ أو إضافة ميزة جديدة. على الرغم من أنه في معظم الحالات، ستحتاج إلى إرسال هذا التصحيح لمطوري المنبع حتى يتم إصلاح الخطأ أو إضافة الميزة في المصدر.

❖ لتجميعها مع خيارات مختلفة (على افتراض أن هناك أسباباً جيدة لعدم قيام Kali بتجميعها مع هذه الخيارات، وإلا قد يكون من الأفضل مناقشة ذلك مع مطوري Kali لمعرفة ما إذا كان يمكنهم تمكين الخيارات المطلوبة).

على النقيض من ذلك، إليك بعض الأسباب السيئة لتعديل حزمة مع اقتراحات حول كيفية معالجة مشكلتك:

❖ لتعديل ملف التكوين. لديك العديد من الخيارات الأفضل مثل استخدام إدارة التكوين لتثبيت ملف تكوين معدّل تلقائيًا أو تثبيت حزمة تكوين ستضع ملفًا في مجلد التكوين (عند توفره) أو سيؤدي إلى تحويل ملف التكوين الأصلي.
❖ للتحديث إلى إصدار أحدث من المصدر. مرة أخرى، من الأفضل العمل مع المطورين لتحديث الحزمة مباشرة في دبيان أو كالي. مع نموذج الإصدار المتداول، تكون التحديثات سريعة إلى حد ما للوصول إلى المستخدمين النهائيين.

من بين جميع الحزم المتاحة، هناك بعض اللبنات الأساسية لـ Kali Linux والتي قد تكون مثيرة للاهتمام في بعض المواقف:

❖ kali-meta: تقوم حزمة المصدر هذه ببناء جميع حزم kali-linux-* meta ولا سيما kali-linux-full، التي تحدد الحزم المثبتة في صورة Kali Linux ISO الافتراضية.
❖ desktop-base: تحتوي حزمة المصدر هذه على ملفات متنوعة يتم استخدامها افتراضياً في عمليات تثبيت سطح المكتب. ضع في اعتبارك طلب هذه الحزمة إذا كنت ترغب في إظهار العلامة التجارية لمؤسستك في الخلفية الافتراضية أو تغيير مظهر سطح المكتب.

kali-menu: تحدد هذه الحزمة بنية قائمة كالي وتوفر ملفات سطح المكتب لجميع التطبيقات التي يجب إدراجها في قائمة كالي.

٢.٣.١٠. إنشاء حزم التكوين

الآن بعد أن تطرقنا إلى إقلاع PXE وناقشنا إدارة التكوين بـ SaltStack بالإضافة إلى تفرع الحزمة، حان الوقت لملء هذه العمليات في مثال عملي وتوسيع السيناريو عن طريق إنشاء حزمة تكوين مخصصة لنشر تكوين مخصص على أجهزة متعددة نصف آلي.

في هذا المثال، ستقوم بإنشاء حزمة مخصصة تقوم بإعداد واستخدام مستودع الحزم الخاص بك ومفتاح توقيع GnuPG، وتوزيع تهيئة SaltStack، ودفع خلفية مخصصة، وتوفير إعدادات سطح المكتب الافتراضية بطريقة موحدة لجميع عمليات تثبيت Kali.

قد تبدو هذه مهمة شاقة (خاصة إذا نظرت عبر مجلد Debian New Maintainer) ولكن لحسن حظنا، فإن حزمة التهيئة هي في الأساس أرشيف ملفات متطور وتحويلها إلى حزمة أمر سهل إلى حد ما.

إلقاء نظرة على عينة حزمة

إذا كنت ترغب في النظر إلى حزمة حقيقية هي في الأساس حزمة تكوين، فكر في حزمة kali-defaults. ليس الأمر بسيطًا مثل العينة في هذا القسم، ولكنه يحتوي على جميع الخصائص ذات الصلة، بل ويستخدم بعض التقنيات المتقدمة (مثل **dpkg-divert**) لاستبدال الملفات المقدمة بالفعل من الحزم الأخرى.

ستحتوي حزمة *offsec-defaults* على عدد قليل من الملفات:

/etc/apt/sources.list.d/offsec.list:

إدخال sources.list لـ APT، مما يتيح مستودع الحزمة الداخلية للشركة.

/etc/apt/trusted.gpg.d/offsec.gpg:

مفتاح GnuPG المستخدم لتوقيع مستودع الحزمة الداخلية للشركة.

/etc/salt/minion.d/offsec.conf:

ملف تكوين SaltStack للإشارة إلى مكان العثور على Salt master.

/usr/share/images/offsec/background.png:

صورة خلفية جميلة مع شعار Offensive Security.

/usr/share/glib-2.0/schemas/90_offsec-defaults.gschema.override:

ملف يقدم إعدادات افتراضية بديلة لسطح مكتب جنوم.

أولاً، قم بإنشاء مجلد offsec-defaults-1.0 ووضع جميع الملفات في هذا المجلد. ثم قم بتشغيل **dh_make --native** (من حزمة dh-make) لإضافة تعليمات تعبئة دبيان، والتي سيتم تخزينها في المجلد الفرعي **debian**:

```
$ mkdir offsec-defaults-1.0; cd offsec-defaults-1.0
$ dh_make --native
```

Type of package: (single, indep, library, python)

[s/i/l/p]? i

```
Email-Address       : buxy@kali.org
License             : gpl3
Package Name        : offsec-defaults
Maintainer Name     : Raphaël Hertzog
Version             : 1.0
Package Type        : indep
Date                : Thu, 16 Jun 2016 18:04:21 +0200
Are the details correct? [Y/n/q] y
Currently there is not top level Makefile. This may require additional tuning
Done. Please edit the files in the debian/ subdirectory now.
```

أولاً، تتم مطالبتك بنوع الحزمة. في المثال، اخترنا *indep*، مما يشير إلى أن حزمة المصدر هذه ستنشئ حزمة ثنائية واحدة يمكن مشاركتها عبر جميع البنى (**Architecture: all**). يعمل *single* كنظير، وينتج حزمة ثنائية واحدة تعتمد على البنية المستهدفة (**Architecture: any**). في هذه الحالة، يكون indep أكثر ملاءمة؛ لأن الحزمة تحتوي فقط على ملفات نصية ولا تحتوي على برامج ثنائية، بحيث يمكن استخدامها بشكل مشابه على أجهزة الحاسوب من جميع الهياكل. يعتبر نوع المكتبة "*library*" مفيدًا للمكتبات المشتركة؛ نظرًا لأنها تحتاج إلى اتباع قواعد تغليف صارمة. بطريقة مماثلة، يجب أن تقتصر *python* على وحدات Python.

اسم المشرف وعنوان بريده الإلكتروني

ستبحث معظم البرامج المتعلقة بصيانة الحزمة عن اسمك وعنوان بريدك الإلكتروني في متغيرات البيئة DEBFULLNAME و DEBEMAIL أو EMAIL. يمنع تعريفها، مرة واحدة وإلى الأبد، إعادة كتابتها عدة مرات. إذا كانت الصدفة الإفتراضية الخاصة بك هي Bash، فهي مسألة بسيطة تتمثل في إضافة السطرين التاليين في ملف **bashrc./~** الخاص بك. فمثلا:

```
export EMAIL="buxy@kali.org"
export DEBFULLNAME="Raphael Hertzog"
```

قام الأمر `dh_make` بإنشاء مجلد فرعي **debian** يحتوي على العديد من الملفات. بعضها مطلوب، ولا سيما **rules**، و**control**، و**changelog**، و**copyright**. الملفات ذات الامتداد **ex.** هي أمثلة للملفات التي يمكن استخدامها بتعديلها وإزالة الامتداد. عندما لا تكون هناك حاجة إليها، نوصي بإزالتها. يجب الاحتفاظ بالملف **compat**، نظراً لأنه مطلوب من أجل الأداء الصحيح لمجموعة برامج *debhelper* (تبدأ جميعها ببادئة **_dh**) المستخدمة في المراحل المختلفة من عملية بناء الحزمة.

يجب أن يحتوي ملف **copyright** على معلومات حول مؤلفي المستندات المضمنة في الحزمة، والترخيص ذي الصلة. إذا كان الترخيص الافتراضي المحدد بواسطة **dh_make** لا يناسبك، فيجب عليك تعديل هذا الملف. فيما يلي النسخة المعدلة من ملف copyright:

Format: https://www.debian.org/doc/packaging-manuals/copyright-format/1.0/

Upstream-Name: offsec-defaults

Files: *

Copyright: 2016 Offensive Security

License: GPL-3.0+

License: GPL-3.0+

along with this program. If not, see <https://www.gnu.org/licenses/>.

.

On Debian systems, the complete text of the GNU General

Public License version 3 can be found in "/usr/share/common-licenses/GPL-3".

ملف **changelog** الافتراضي مناسب بشكل عام، يجب أن يكون استبدال "Initial release" بشرح أكثر تفصيلاً كافياً:

offsec-defaults (1.0) unstable; urgency=medium

* Add salt minion's configuration file.

* Add an APT's sources.list entry and an APT's trusted GPG key.

* Override the gsettings schema defining the background picture.

-- Raphaël Hertzog <buxy@kali.org> Thu, 16 Jun 2016 18:04:21 +0200

في المثال، سنقوم بإجراء تغييرات على ملف التحكم "**control**". سنقوم بتغيير حقل **Section** لإخفاء وإزالة حقول **Homepage** و **Vcs-Git** و **Vcs-Browser**. أخيرًا، سنملأ حقل **Description**:

```
Source: offsec-defaults
Section: misc
Priority: optional
Maintainer: Raphaël Hertzog <buxy@kali.org>
Build-Depends: debhelper (>= 9)
Standards-Version: 3.9.8

Package: offsec-defaults
Architecture: all
Depends: ${misc:Depends}
Description: Default settings for Offensive Security
 This package contains multiple files to configure computers
 owned by Offensive Security.
 .
 It notably modifies:
  - APT's configuration
```

- salt-minion's configuration

- the default desktop settings

يحتوي ملف **rules** عادةً على مجموعة من القواعد المستخدمة لتكوين البرنامج وتثبيته وتثبيته في دليل فرعي مخصص (يسمى بعد الحزمة الثنائية التي تم إنشاؤها). يتم بعد ذلك أرشفة محتويات هذا المجلد الفرعي ضمن حزمة دبيان كما لو كانت جذر نظام الملفات. في هذه الحالة، سيتم تثبيت الملفات في المجلد الفرعي **/debian/offsec-defaults**. على سبيل المثال، للحصول على حزمة تثبيت **/etc/apt/sources.list.d/offsec.list**، قم بتثبيت الملف في **debian/offsec-defaults/etc/apt/sources.list.d/offsec.list**. يتم استخدام ملف **rules** كملف **Makefile**، مع بعض الأهداف القياسية (بما في ذلك **clean** و**binary**، تستخدم على التوالي لتنظيف المجلد المصدر وإنشاء الحزمة الثنائية).

ما هو ملف Makefile؟

ربما تكون قد لاحظت الرسالة المتعلقة بـ **Makefile** المفقود في نهاية إخراج **dh_make** وذكر تشابهها مع ملف **rules**. ملف **Makefile** هو ملف نصي يستخدمه برنامج **make**، يصف قواعد كيفية إنشاء مجموعة من الملفات من بعضها البعض في شجرة من التبعيات. على سبيل المثال، يمكن بناء برنامج من مجموعة من الملفات المصدر. يصف ملف **Makefile** هذه القواعد بالتنسيق التالي:

```
target: source1 source2 ...
        command1
        command2
```

تفسير مثل هذه القاعدة هو كما يلي: إذا كان أحد ملفات **source*** أحدث من الملف **target**، فيجب إنشاء الهدف، باستخدام **command1** و **command2**.

لاحظ أن أسطر الأوامر يجب أن تبدأ بحرف tabs؛ لاحظ أيضًا أنه عندما يبدأ سطر الأوامر بحرف شرطة (-)، فإن فشل الأمر لا يقاطع العملية بأكملها.

على الرغم من أن هذا الملف هو جوهر العملية، إلا أنه يحتوي على الحد الأدنى فقط لتشغيل مجموعة قياسية من الأوامر التي توفرها أداة `debhelper`. هذا هو الحال بالنسبة للملفات التي تم إنشاؤها بواسطة `dh_make`. لتثبيت معظم ملفاتك، نوصي بتهيئة سلوك الأمر `dh_install` عن طريق إنشاء ملف **debian/offsec-defaults.install** التالي:

apt/offsec.list etc/apt/sources.list.d/

apt/offsec.gpg etc/apt/trusted.gpg.d/

salt/offsec.conf etc/salt/minion.d/

images/background.png usr/share/images/offsec/

يمكنك أيضًا استخدام هذا لتثبيت ملف إلغاء gsettings لكن debhelper يوفر أداة مخصصة لهذا (**dh_installgsettings**) حتى تتمكن من الاعتماد عليه. أولاً، ضع إعداداتك في **debian/offsec-defaults.gsettings-override**:

```
[org.gnome.desktop.background]
picture-options='zoom'
picture-uri='file:///usr/share/images/offsec/background.png'
```

بعد ذلك، قم بإلغاء استدعاء **dh_installgsettings** في **debian/rules** لزيادة الأولوية إلى المستوى المتوقع لإلغاء المؤسسة (وهو ٩٠ وفقًا للصفحة اليدوية):

```
#!/usr/bin/make -f

%:
	dh $@

override_dh_installgsettings:
	dh_installgsettings --priority=90
```

عند هذه النقطة، الحزمة المصدر جاهزة. كل ما تبقى للقيام به هو إنشاء الحزمة الثنائية بنفس الطريقة المستخدمة سابقًا لإعادة بناء الحزم: قم بتشغيل الأمر **dpkg-buildpackage -us -uc** من داخل مجلد **offsec-defaults-1.0**:

```
$ dpkg-buildpackage -us -uc
dpkg-buildpackage: info: source package offsec-defaults
dpkg-buildpackage: info: source version 1.0
```

```
dpkg-buildpackage: info: source distribution unstable
dpkg-buildpackage: info: source changed by Raphaël Hertzog <buxy@kali.org>
dpkg-buildpackage: info: host architecture amd64
 dpkg-source --before-build offsec-defaults-1.0
 fakeroot debian/rules clean
dh clean
   dh_testdir
   dh_auto_clean
   dh_clean
 dpkg-source -b offsec-defaults-1.0
dpkg-source: info: using source format '3.0 (native)'
dpkg-source: info: building offsec-defaults in offsec-defaults_1.0.tar.xz
dpkg-source: info: building offsec-defaults in offsec-defaults_1.0.dsc
 debian/rules build
dh build
   dh_testdir
   dh_update_autotools_config
   dh_auto_configure
```

```
   dh_auto_build
   dh_auto_test
 fakeroot debian/rules binary
dh binary
   dh_testroot
   dh_prep
   dh_auto_install
   dh_install
   dh_installdocs
   dh_installchangelogs
   debian/rules override_dh_installgsettings
make[1]: Entering directory '/home/rhertzog/kali/kali-book/samples/offsec-defaults-1.0'
dh_installgsettings --priority=90
make[1]: Leaving directory '/home/rhertzog/kali/kali-book/samples/offsec-defaults-1.0'
   dh_perl
   dh_link
   dh_strip_nondeterminism
```

dh_compress

dh_fixperms

dh_installdeb

dh_gencontrol

dh_md5sums

dh_builddeb

dpkg-deb: building package 'offsec-defaults' in '../offsec-defaults_1.0_all.deb'.

dpkg-genchanges >../offsec-defaults_1.0_amd64.changes

dpkg-genchanges: info: including full source code in upload

dpkg-source --after-build offsec-defaults-1.0

dpkg-buildpackage: info: full upload; Debian-native package (full source is included)

٣.٣.١. إنشاء مستودع حزمة لـ APT

الآن بعد أن أصبح لديك حزمة مخصصة، يمكنك توزيعها من خلال مستودع حزمة APT. استخدم **reprepro** لإنشاء المستودع المطلوب وملئه. هذه الأداة قوية إلى حد ما، ومن المؤكد أن صفحتها اليدوية تستحق القراءة.

عادة ما يتم استضافة مستودع الحزمة على الخادم. لفصلها بشكل صحيح عن الخدمات الأخرى التي تعمل على الخادم، من الأفضل إنشاء مستخدم مخصص لهذه الخدمة. في حساب المستخدم المخصص، ستكون قادرًا على استضافة ملفات المستودع وأيضًا مفتاح GnuPG الذي سيتم استخدامه لتوقيع مستودع الحزمة:

```
# apt install reprepro gnupg
[...]
# adduser --system --group pkgrepo
Adding system user 'pkgrepo' (UID 136) ...
Adding new group 'pkgrepo' (GID 142) ...
Adding new user 'pkgrepo' (UID 136) with group 'pkgrepo' ...
Creating home directory '/home/pkgrepo' ...
# chown pkgrepo $(tty)
# su - -s /bin/bash pkgrepo
$ gpg --gen-key
```

gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc.

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/pkgrepo/.gnupg' created

gpg: new configuration file '/home/pkgrepo/.gnupg/dirmngr.conf' created

gpg: new configuration file '/home/pkgrepo/.gnupg/gpg.conf' created

gpg: keybox '/home/pkgrepo/.gnupg/pubring.kbx' created

Note: Use "gpg --full-gen-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Offensive Security Repository Signing Key

Email address: repoadmin@offsec.com

You selected this USER-ID:

"Offensive Security Repository Signing Key <repoadmin@offsec.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o

We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.

[...]

gpg: /home/pkgrepo/.gnupg/trustdb.gpg: trustdb created

gpg: key B4EF2D0D marked as ultimately trusted

gpg: directory '/home/pkgrepo/.gnupg/openpgp-revocs.d' created

gpg: revocation certificate stored as '/home/pkgrepo/.gnupg/openpgp-revocs.d/F8FE22F74F1B714E38DA6181B27F74F7B4EF2D0D.rev'

public and secret key created and signed.

gpg: checking the trustdb

gpg: marginals needed: 3 completes needed: 1 trust model: PGP

gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u

pub rsa2048/B4EF2D0D 2016-06-17 [S]

Key fingerprint = F8FE 22F7 4F1B 714E 38DA 6181 B27F 74F7 B4EF 2D0D

uid [ultimate] Offensive Security Repository Signing Key <repoadmin@offsec.com>

sub rsa2048/38035F38 2016-06-17 []

لاحظ أنه عندما يُطلب منك عبارة مرور، يجب عليك إدخال قيمة فارغة (والتأكيد على أنك لا تريد حماية مفتاحك الخاص) لأنك تريد أن تكون قادرًا على توقيع المستودع بشكل غير تفاعلي. لاحظ أيضًا أن **gpg** يتطلب حق الوصول للكتابة إلى المحطة الطرفية حتى تتمكن من المطالبة بعبارة مرور بشكل آمن: لهذا السبب قمت بتغيير ملكية المحطة الافتراضية (التي يملكها الجذر منذ اتصالك في البداية بهذا المستخدم) قبل بدء تشغيل shell كـ **pkgrepo**.

الآن يمكنك البدء في إعداد المستودع. مجلد مخصص ضروري لـ **reprepro** وداخل هذا المجلد يجب عليك إنشاء ملف **conf/distributions** يوثق التوزيعات المتوفرة في مستودع الحزمة:

```
$ mkdir -p reprepro/conf
$ cd reprepro
$ cat >conf/distributions <
```

الحقول المطلوبة هي **Codename**، والتي تعطي اسم التوزيع، و**Architectures**، والتي تشير إلى البنيات التي ستكون متاحة في التوزيعة (والمقبولة على جانب الإدخال)، و**Components**، والتي تشير إلى المكونات المختلفة المتاحة في التوزيعة (المكونات هي نوع من القسم الفرعي للتوزيعة، والذي يمكن تمكينه بشكل منفصل في قائمة مصادر APT). إن حقول **Origin** و**Description** مفيدة تمامًا ويتم نسخها كما هي في ملف **Release**. يطلب حقل **SignWith** من **reprepro** توقيع المستودع باستخدام مفتاح GnuPG الذي تم إدراج معرفه (ضع البصمة الكاملة هنا لضمان استخدام المفتاح الصحيح، وليس اصطدام آخر بالمعرف القصير). إعداد **AlsoAcceptFor** ليس مطلوبًا ولكنه يجعل من الممكن معالجة ملفات **changes.** التي يحتوي حقل توزيعها على قيمة مدرجة هنا (بدون هذا، لن يقبل سوى اسم كود "codename" التوزيع في هذا الحقل).

باستخدام هذا الإعداد الأساسي، يمكنك السماح لـ **reprepro** بإنشاء مستودع فارغ:

```
$ reprepro export
Exporting indices...
$ find .
.
./db
./db/version
./db/references.db
./db/contents.cache.db
./db/checksums.db
./db/packages.db
./db/release.caches.db
./conf
./conf/distributions
./dists
./dists/offsec-internal
./dists/offsec-internal/Release.gpg
./dists/offsec-internal/Release
./dists/offsec-internal/main
```

./dists/offsec-internal/main/source

./dists/offsec-internal/main/source/Release

./dists/offsec-internal/main/source/Sources.gz

./dists/offsec-internal/main/binary-amd64

./dists/offsec-internal/main/binary-amd64/Packages

./dists/offsec-internal/main/binary-amd64/Release

./dists/offsec-internal/main/binary-amd64/Packages.gz

./dists/offsec-internal/main/binary-i386

./dists/offsec-internal/main/binary-i386/Packages

./dists/offsec-internal/main/binary-i386/Release

./dists/offsec-internal/main/binary-i386/Packages.gz

./dists/offsec-internal/InRelease

كما ترى، قام reprepro بإنشاء معلومات تعريف المستودع في مجلد فرعي dists. كما قام بتهيئة قاعدة بيانات داخلية في مجلد فرعي **db**.

حان الوقت الآن لإضافة الحزمة الأولى الخاصة بك. أولاً، انسخ الملفات التي تم إنشاؤها من خلال إنشاء حزم offsec المختلفة:

(**offsec-defaults_1.0.dsc**, **offsec-defaults_1.0.tar.xz**, **offsec-defaults_1.0_all.deb**, and **offsec-defaults_1.0_amd64.changes**)

داخل **tmp/** على الخادم الذي يستضيف مستودع الحزمة واطلب من reprepro تضمين الحزمة:

```
$ reprepro include offsec-internal /tmp/offsec-defaults_1.0_amd64.changes
```

Exporting indices...

```
$ find pool
```

pool

pool/main

pool/main/o

pool/main/o/offsec-defaults

pool/main/o/offsec-defaults/offsec-defaults_1.0.dsc

pool/main/o/offsec-defaults/offsec-defaults_1.0.tar.xz

pool/main/o/offsec-defaults/offsec-defaults_1.0_all.deb

كما ترى، أضاف الملفات إلى تجمع الحزمة الخاص به في مجلد فرعي **pool**.

dists ومجلدات **pool** هي المجلدات التي تحتاج إلى إتاحتها (بشكل عام) عبر HTTP لإنهاء إعداد مستودع APT الخاص بك. تحتوي على جميع الملفات التي تريد APT تنزيلها.

بافتراض رغبتك في استضافة هذا على مضيف افتراضي باسم **pkgrepo.offsec.com**، يمكنك إنشاء ملف تكوين Apache التالي وحفظه في **/etc/apache2/sites-available/pkgrepo.offsec.com.conf** وتمكينه بواسطة: **a2ensite pkgrepo.offsec.com**):

```
    ServerName pkgrepo.offsec.com
    ServerAdmin repoadmin@offsec.com

    ErrorLog /var/log/apache2/pkgrepo.offsec.com-error.log
    CustomLog /var/log/apache2/pkgrepo.offsec.com-access.log "%h %l %u %t "%r" %>s %O"
    DocumentRoot /home/pkgrepo/reprepro

        Options Indexes FollowSymLinks MultiViews
        Require all granted
        AllowOverride All
```

وسيبدو إدخال sources.list المقابل لإضافته إلى الأجهزة التي تحتاج إلى حزم من هذا المستودع كما يلي:

```
deb http://pkgrepo.offsec.com offsec-internal main

# Enable next line if you want access to source packages too
# deb-src http://pkgrepo.offsec.com offsec-internal main
```

تم نشر الحزمة الخاصة بك الآن ويجب أن تكون متاحة للمضيفين المتصلين بالشبكة.

على الرغم من أن هذا كان إعدادًا طويلاً، فقد اكتمل الآن "الرفع الثقيل". يمكنك تشغيل أجهزتك المتصلة بالشبكة عبر PXE، وتثبيت نسخة مخصصة من Kali Linux بدون تفاعل بفضل السعر الذي يتم توصيله عبر الشبكة، وتكوين SaltStack لإدارة التكوينات الخاصة بك (والتحكم في التوابع!)، وإنشاء حزم مخصصة متشعبة، وتوزيع هذه الحزم من خلال مستودع الحزمة الخاصة. وهذا يوفر إدارة مركزية وتحكمًا على مستوى المؤسسة في العديد من عمليات تثبيت Kali Linux. باختصار، يمكنك الآن نشر أنظمة Kali عالية الأمان بسرعة والتي تم تكوينها مسبقًا وفقًا لاحتياجاتك الخاصة والاحتفاظ بها متزامنة بفضل تثبيت Kali (شبه التلقائي) لجميع تحديثات الحزمة.

٤.١٠. ملخص

يمتد Kali Linux إلى ما بعد سطح المكتب إلى عمليات النشر على نطاق متوسط أو كبير وحتى إلى مستوى المؤسسة. في هذا الفصل، قمنا بتغطية كيفية مركزة إدارة العديد من مستودعات Kali باستخدام SaltStack، مما يتيح لك نشر أنظمة Kali عالية الأمان التي تم تكوينها مسبقًا لتلبية احتياجاتك الخاصة بسرعة. كشفنا أيضًا عن كيفية إبقائها متزامنة بفضل تثبيت Kali (شبه التلقائي) لتحديثات الحزمة.

ناقشنا تفرع الحزمة، والذي يسمح لك بإنشاء حزم المصدر القابلة للتوزيع المخصصة الخاصة بك.

باختصار، دعنا نراجع الخطوات الرئيسية المطلوبة لتأسيس Salt masters وminions، والتي تتيح لك التحكم عن بعد وتكوين المضيفين البعيدين.

نصائح تلخيصية:

إقلاع الجهاز من الشبكة باستخدام PXE، بخادم ملفات TFTP على الأقل، وخادم DHCP/BOOTP (وخادم ويب للتنبؤ باستخدام debconf). يتعامل *dnsmasq* مع كل من DHCP و TFTP، ويأتي خادم الويب apache2 مثبتاً مسبقًا (ولكن معطل) على Kali.

يغطي دليل تثبيت ديبان إعداد خادم isc-dhcp-server و tftpd-hpa لإقلاع PXE:

https://www.debian.org/releases/stable/amd64/ch04s05.html

تم تكوين dnsmasq من خلال **/etc/dnsmasq.conf**. يتكون التكوين الأساسي من بضعة خطوط رئيسية فقط:

```
# Network interface to handle
interface=eth0
# DHCP options
# IP range to allocate
dhcp-range=192.168.101.100,192.168.101.200,12h
# Gateway to announce to clients
dhcp-option=option:router,192.168.101.1
# DNS servers to announce to clients
dhcp-option=option:dns-server,8.8.8.8,8.8.4.4
# Boot file to announce to clients
dhcp-boot=pxelinux.0
# TFTP options
enable-tftp
# Directory hosting files to serve
tftp-root=/tftpboot/
```

فك حزم ملفات تثبيت التثبيت 32bit (i386) و 64bit (amd64) أو القياسية أو الرسومية (gtk) من أرشيف Kali إلى / tftpboot /. يمكن العثور على الأرشيف هنا:

http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images/netboot/gtk/netboot.tar.gz

http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images/netboot/netboot.tar.gz

http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images/netboot/gtk/netboot.tar.gz

http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images/netboot/netboot.tar.gz

```
# mkdir /tftpboot
# cd /tftpboot
# wget http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images/netboot/netboot.tar.gz
# tar xf netboot.tar.gz
```

قم بتعديل txt.cfg اختيارياً إلى المعلمات المتوقعة أو المهلات المخصصة. انظر القسم ٣.٤، "التثبيتات غير المراقبة". بعد ذلك، يمكنك الاستفادة من أدوات إدارة التكوين لإدارة الأجهزة أو تكوين أجهزة الكمبيوتر البعيدة لأي حالة مرغوبة.

SaltStack هي خدمة إدارة تكوين مركزية: يدير سيد الملح العديد من توابع الملح. قم بتثبيت حزمة الملح الرئيسي على خادم يمكن الوصول إليه وملح minion على المضيفين المُدارين.

قم بتحرير الملف **/etc/salt/minion** بتنسيق YAML وقم بتعيين المفتاح الرئيسي لاسم DNS (أو عنوان IP) الخاص بـSalt master.

تعيين معرّف العميل الفريد في **/etc/salt/minion_id**:

```
minion# echo kali-scratch >/etc/salt/minion_id
minion# systemctl enable salt-minion
minion# systemctl start salt-minion
```

سيتبع تبادل المفتاح. بالنسبة للسيد، اقبل مفتاح تعريف العميل. ستكون الاتصالات اللاحقة تلقائية:

```
master# systemctl enable salt-master
master# systemctl start salt-master
master# salt-key --list all
```

Accepted Keys:

Denied Keys:

Unaccepted Keys:

kali-scratch

Rejected Keys:

```
master# salt-key --accept kali-scratch
```

The following keys are going to be accepted:

Unaccepted Keys:

kali-scratch

Proceed? [n/Y] y

Key for minion kali-scratch accepted.

بمجرد توصيل التوابع، يمكنك تنفيذ الأوامر عليها من السيد. أمثلة:

```
master# salt '*' test.ping
kali-scratch:
True
kali-master:
True
master# salt kali-scratch cmd.shell 'uptime; uname
-a'
master# salt kali-scratch sys.doc'
master# salt '*' service.enable ssh
[...]
master# salt '*' service.start ssh
[...]
master# salt '*' pkg.refresh_db
[...]
master# salt '*' pkg.upgrade dist_upgrade=True
server# salt '*' cmd.shell 'pkill -f dnmap_client'
```

يمكن العثور على القائمة الكاملة لوحدات التنفيذ على:

https://docs.saltstack.com/en/latest/ref/modules/all/index.html

استخدم ملفات Salt State (قوالب التكوين القابلة لإعادة الاستخدام) لجدولة الإجراءات، وجمع البيانات، وتنظيم تسلسل العمليات على التوابع المتعددة، وتوفير أنظمة سحابية وإخضاعها للإدارة، والمزيد. وفر الوقت باستخدام صيغ salt المحددة مسبقًا:

https://docs.saltstack.com/en/latest/topics/development/conventions/formulas.html

عندما يحين الوقت لـhook حزمة، قرر أولاً ما إذا كانت مهمة تحتاج إلى معالجتها. هناك مزايا وعيوب كبيرة. راجعها بعناية. حزم kali-meta وdesktop-base وkali-menu خيارات مثيرة للاهتمام ومحتملة. يمكن أن تكون عملية التزوير حزمة شاقة ويصعب تلخيصها.

الآن بعد أن قمنا بتغطية جميع القواعد من حيث التثبيت والتكوين والتخصيص والنشر لـ Kali Linux، فلننتقل إلى دور Kali Linux في مجال أمن المعلومات.

التمرين الأول للفصل العاشر - تكوين salt masterو minion.

لتكوين salt master و minion استخدم أوامر مشابهة لتلك. لاحظ أنه يجب إصدار بعض الأوامر على master، وبعضها العميل "minion" (أو التابع "slave") كما هو موضح في موجهات الأوامر.

أولاً، يجب عليك تثبيت حزمة salt-master على خادم يمكن الوصول إليه من قبل جميع المضيفين الذين ترغب في إدارتهم وsalt-minion على المضيفين الذين ترغب في إدارتهم. سيتطلب هذا جهازين، أو VM. قم بإعداد واحد أولاً. من أجل العرض التوضيحي، يمكنك استخدام اثنين من مثيل الإقلاع المباشر "*live boot instance*".

على الجهاز الذي تريده أن يكون السيد "master":

```
master# apt-get install salt-master
```

إذا كنت تستخدم صورتك من التمرين الخامس للفصل التاسع فيمكنك استخدام ذلك كعميل لتثبيت صورة iso. بخلاف ذلك، قم بتدوير VM مباشر آخر للminion وتنفيذ **apt-get install salt-minion**:

```
minion# dhclient eth0 #أو أي إعداد شبكة آخر تفضله
minion# apt-get install salt-minion
```

بعد ذلك، يجب إخبار كل عميل بمكان العثور على سيده. ما عليك سوى تعديل **/etc/salt/minion** وتعيين المفتاح الرئيسي لاسم DNS (أو عنوان IP) الخاص salt master:

```
minion# nano /etc/salt/minion
minion# grep ^master /etc/salt/minion
master: 192.168.122.105
```

لكل عميل معرف فريد مخزن في **/etc/salt/minion_id**، والذي يتم تعيينه افتراضياً على اسم المضيف الخاص به. سيتم استخدام معرف العميل هذا في قواعد التكوين وعلى هذا النحو، من المهم ضبطه بشكل صحيح قبل أن يفتح العميل اتصاله بالسيد:

```
minion# echo kali-scratch >/etc/salt/minion_id
minion# systemctl enable salt-minion
minion# systemctl start salt-minion
```

عند تشغيل خدمة salt-minion، ستحاول الاتصال salt master لتبادل بعض مفاتيح التشفير. على الجانب الرئيس "master"، يجب عليك قبول المفتاح الذي يستخدمه العميل لتعريف نفسه للسماح بالاتصال. ستكون الاتصالات اللاحقة تلقائية:

```
master# systemctl enable salt-master
master# systemctl start salt-master
master# salt-key --list all
master# salt-key --accept kali-scratch
```

بمجرد أن يتم توصيل التوابع، يمكنك تنفيذ الأوامر عليها من الرئيس. أمثلة:

```
master# salt kali-scratch cmd.shell 'uptime; uname -a'
master# salt kali-scratch sys.doc disk.usage
master# salt '*' service.enable ssh
master# salt '*' service.start ssh
master# salt '*' pkg.refresh_db
master# salt '*' pkg.upgrade dist_upgrade=True
```

التمرين الثاني للفصل العاشر - إنشاء مستودع كالي

إنشاء مستودع كالي. قم باستضافة الحزم التي قمت بإنشائها فيها (SET, kali-menu, kernel packages).

الإجابة:

الآن بعد أن أصبح لديك حزمة مخصصة، يمكنك توزيعها من خلال مستودع حزمة APT. استخدم **reprepro** لإنشاء المستودع المطلوب وملئه.

عادة ما يتم استضافة مستودع الحزمة على الخادم. لفصلها بشكل صحيح عن الخدمات الأخرى التي تعمل على الخادم، من الأفضل إنشاء مستخدم مخصص لهذه الخدمة. في حساب المستخدم المخصص، ستكون قادرًا على استضافة ملفات المستودع وأيضًا مفتاح GnuPG الذي سيتم استخدامه لتوقيع مستودع الحزمة:

```
apt install reprepro gnupg2

adduser --system --group pkgrepo

chown pkgrepo $(tty) # gpg requires write access to
the terminal

su - -s /bin/bash pkgrepo

gpg2 --gen-key # Don't enter password
```

لاحظ أننا لا ندخل عبارة مرور حتى نتمكن من تسجيل الدخول بشكل غير تفاعلي.

بعد ذلك، قم بإعداد بنية المستودع. مجلد مخصص ضروري لـ reprepro وداخل هذا المجلد يجب عليك إنشاء ملف conf/distributions للتوريدات يوثق التوزيعات المتوفرة في مستودع الحزمة:

```
mkdir -p reprepro/conf
cd reprepro
```

بعد ذلك، قم بتعديل **conf/distributions.**

```
nano conf/distributions
```

.. لتبدو هكذا:

```
Codename: offsec-internal

AlsoAcceptFor: unstable

Origin: Offensive Security

Description: Offsec's Internal packages

Architectures: source amd64 i386

Components: main

SignWith: F8FE22F74F1B714E38DA6181B27F74F7B4EF2D0D
```

باستخدام هذا الإعداد الأساسي، يمكنك السماح لـ reprepro بإنشاء مستودع فارغ:

```
$ reprepro export
```

اطلب من reprepro تضمين الحزمة. استخدم ملف changes. من الحزمة المخصصة السابقة الخاصة بك!

```
reprepro include offsec-internal /tmp/offsec-defaults_1.0_amd64.changes
```

لاحظ أن reprepro أضاف الملفات إلى مجموعة الحزم الخاصة به في مجلد فرعي للتجمع:

```
find pool
```

الأقراص ومجلدات التجمع هي المجلدات التي تحتاج إلى إتاحتها (بشكل عام) عبر HTTP لإنهاء إعداد مستودع APT الخاص بك. تحتوي على جميع الملفات التي تريد APT تنزيلها.

بافتراض رغبتك في استضافة هذا على مضيف افتراضي باسم pkgrepo.offsec.com، يمكنك إنشاء ملف التكوين ٢ التالي وحفظه في:

/etc/apache2/sites-available/pkgrepo.offsec.com.conf

وتمكينه بواسطة: **a2ensite pkgrepo.offsec.com**:

```
<VirtualHost *:80>
    ServerName pkgrepo.offsec.com
    ServerAdmin repoadmin@offsec.com
```

```
    ErrorLog /var/log/apache2/pkgrepo.offsec.com-error.log
    CustomLog /var/log/apache2/pkgrepo.offsec.com-access.log "%h %l %u %t \"%r\" %>s %O"
    DocumentRoot /home/pkgrepo/reprepro
    <Directory "/home/pkgrepo/reprepro">
        Options Indexes FollowSymLinks MultiViews
        Require all granted
        AllowOverride All
    </Directory>
</VirtualHost>
```

وسيبدو إدخال sources.list المقابل لإضافته إلى الأجهزة التي تحتاج إلى حزم من هذا المستودع كما يلي:

```
deb http://pkgrepo.offsec.com offsec-internal main
# Enable next line if you want access to source packages too
# deb-src http://pkgrepo.offsec.com offsec-internal main
```

تم نشر الحزمة الخاصة بك الآن ويجب أن تكون متاحة للمضيفين المتصلين بالشبكة.

```
pkgrepo@kali:~/ reprepro$gpg2 --export --armor
muts@offsec.com > /tmp/wot.asc
```

```
cat /tmp/wot.asc | apt-key add -
```

```
apt-key list
```

```
apt-key del KEYHERE
```

التمرين الثالث للفصل العاشر - إنشاء حزمة تكوين من البداية.

قم بإنشاء حزمة مخصصة تقوم بإعداد واستخدام مستودع الحزم الخاص بك ومفتاح توقيع GnuPG، وتوزيع تهيئة SaltStack، ودفع خلفية مخصصة، وتوفير إعدادات سطح المكتب الافتراضية بطريقة موحدة لجميع عمليات تثبيت Kali.

ستحتوي هذه الحزمة الافتراضية على عدد قليل من الملفات:

/etc/apt/sources.list.d/offsec.list:

إدخال sources.list لـ APT، مما يتيح مستودع الحزمة الداخلية للشركة.

/etc/apt/trusted.gpg.d/offsec.gpg:

مفتاح GnuPG المستخدم لتوقيع مستودع الحزمة الداخلية للشركة.

/etc/salt/minion.d/offsec.conf:

ملف تكوين SaltStack للإشارة إلى مكان العثور على الصفحة salt master.

/usr/share/images/offsec/background.png:

صورة خلفية جميلة مع شعار Offensive Security.

/usr/share/glib-2.0/schemas/90_offsec-defaults.gschema.override:

ملف يقدم إعدادات افتراضية بديلة لسطح مكتب جنوم.

أولاً، عرف هذه المتغيرات حتى لا تضطر إلى كتابتها عدة مرات:

```
export EMAIL="muts@kali.org"
export DEBFULLNAME="Mati Aharoni"
```

إنشاء مجلد offsec-defaults-1.0 ووضع جميع الملفات في هذا المجلد. ثم قم بتشغيل **dh_make –native** (من حزمة dh-make) لإضافة تعليمات تعبئة دبيان، والتي سيتم تخزينها في مجلد فرعي **debian**:

```
mkdir offsec-defaults-1.0; cd offsec-defaults-1.0
dh_make --native
cd debian
ls -l
```

إزالة ملفات الأمثلة:

```
rm *.ex *.EX *.docs README*
```

قم بتحديث معلومات عنك (المؤلف) في حقوق الطبع والنشر وإلقاء نظرة على التوافق:

```
nano copyright
nano compat
```

بعد ذلك، قم بتحرير ملف **offsec-defaults.install** الخاص بك ...

```
nano offsec-defaults.install
```

... لتضمين **offsec.list** (ملف sources.list)، **offsec.gpg** (مفتاح GnuPG المستخدم لتوقيع مستودع الحزمة الداخلية للشركة)، **offsec.conf** (ملف تكوين SaltStack الذي يشير إلى مكان العثور على Salt master)، وصورة خلفية جميلة:

apt/offsec.list etc/apt/sources.list.d/

apt/offsec.gpg etc/apt/trusted.gpg.d/

salt/offsec.conf etc/salt/minion.d/

images/background.png usr/share/images/offsec/

تحديث ملف **gsettings-override** ...

```
nano offsec-defaults.gsettings-override
```

لتضمين:

```
[org.gnome.desktop.background]
picture-options='zoom'
picture-uri='file:///usr/share/images/offsec/background.png'
```

الآن سنقوم بتحرير:

```
nano rules
```

.. لزيادة الأولوية إلى المستوى المتوقع لإلغاء المؤسسة (وهو ٩٠ طبقًا لصفحة الدليل):

```
#!/usr/bin/make -f

%:
	dh $@

override_dh_installgsettings:
	dh_installgsettings --priority=90
```

قم بإنشاء مجلدات لمراعاة ما قمنا بوضعه في **offsec-defaults.install**. هذا هو المكان الذي تضع فيه أغراضك! (افعلها!)

```
mkdir ../{apt,salt,images}
cd ..
```

عند هذه النقطة، الحزمة المصدر جاهزة. كل ما تبقى للقيام به هو إنشاء الحزمة الثنائية بنفس الطريقة المستخدمة سابقًا لإعادة بناء الحزم: قم بتشغيل الأمر **dpkg-buildpackage -us -uc** من داخل مجلد offsec-defaults-1.0:

```
dpkg-buildpackage -us -uc
```

اختبار الشهادة للفصل العاشر

١. أي مما يلي مطلوب لتثبيت كالي عبر الشبكة على جهاز بدون نظام تشغيل؟

- TFTP
- PXE
- BOOTP
- DHCP
- ليس أي مما يلي
- كل ما يلي

٢. أي من الأوامر التالية سيقوم بتثبيت حزمة dnmap على salt minions؟

- salt ’*’ pkg.install dnmap
- salt ’*’ install dnmap
- salt ’*’ –install dnmap
- salt ’*’ -i dnmap

٣. أي من الأوامر التالية سينشئ حزمة ثنائية وحزمة مصدر غير موقعة مع ملف buildinfo. و changes. غير موقع؟

- dpkg-buildpackage -us -ub
- dpkg-buildpackage -us -uc
- dpkg-build -p -us -ub
- dpkg –build –u

٤. ما هو الأمر المستخدم لإنشاء وإدارة مستودعات ديبان؟

- deb_repo
- pkgrepo
- reprepro
- debrepo

٥. حدد جميع الحقول المطلوبة في ملف تكوين repo:

- Status
- Codename
- Components
- Architectures

٦. ما هو الملف الذي يجب تحديثه على أجهزة العميل التي ترغب في الوصول إلى مستودع مخصص؟

- sources.list
- sources.conf
- repo.conf
- repo.list

الإجابة:

- All of the above.
- salt '*' pkg.install dnmap.
- reprepro.
- Codename, Components, Architectures.
- sources.list

١١. مقدمة إلى التقييمات الأمنية

لقد غطينا العديد من الميزات الخاصة بـ Kali Linux حتى هذه اللحظة، لذا يجب أن يكون لديك فهم قوي لما يجعل Kali مميزًا وكيفية إنجاز عدد من المهام المعقدة.

ولكن قبل استخدام Kali، هناك بعض المفاهيم المتعلقة بالتقييمات الأمنية التي يجب أن تفهمها. في هذا الفصل، سنقدم هذه المفاهيم لمساعدتك على البدء وتقديم مراجع ستساعدك إذا كنت بحاجة إلى استخدام Kali لإجراء تقييم أمني.

بادئ ذي بدء، يجدر تخصيص بعض الوقت لاستكشاف ما يعنيه "الأمان "security"" بالضبط عند التعامل مع أنظمة المعلومات. عند محاولة تأمين نظام معلومات، فإنك تركز على ثلاث سمات أساسية للنظام:

السرية "*Confidentiality*": هل يمكن للجهات الفاعلة التي لا ينبغي أن يكون لديها وصول إلى النظام أو المعلومات الوصول إلى النظام أو المعلومات؟

النزاهة "*Integrity*": هل يمكن تعديل البيانات أو النظام بطريقة غير مقصودة؟

الإتاحة "*Availability*": هل يمكن الوصول إلى البيانات أو النظام متى وكيف يكون المقصود؟

تشكل هذه المفاهيم معًا ثلاثي CIA (السرية والنزاهة والتوافر) وهي إلى حد كبير العناصر الأساسية التي ستركز عليها عند تأمين نظام لجزء من النشر القياسي أو الصيانة أو التقييم.

من المهم أيضًا ملاحظة أنه في بعض الحالات، قد تكون مهتمًا أكثر بكثير من جانب واحد من ثالوث CIA من غيرها. على سبيل المثال، إذا كانت لديك مجلة شخصية تحتوي على أفكارك الأكثر سرية، فقد تكون سرية المجلة أكثر أهمية بالنسبة لك من النزاهة أو التوفر. بعبارة أخرى، قد لا تقلق بشأن ما إذا كان بإمكان أي شخص الكتابة إلى المجلة (بدلاً من قراءتها) أو ما إذا كانت المجلة متاحة دائمًا أم لا. من ناحية أخرى، إذا كنت تقوم بتأمين نظام يتتبع الوصفات الطبية، فستكون سلامة البيانات أكثر أهمية. في حين أنه من المهم منع الأشخاص الآخرين من قراءة الأدوية التي يستخدمها شخص ما ومن المهم أن تتمكن من الوصول إلى قائمة الأدوية هذه، إذا تمكن شخص ما من تغيير محتويات النظام (تغيير النزاهة أو السلامة "integrity")، فقد يؤدي ذلك نتائج تهدد الحياة.

عند تأمين نظام واكتشاف مشكلة، سيتعين عليك التفكير في أي من هذه المفاهيم الثلاثة، أو أي مجموعة منها، تندرج المشكلة فيها. يساعدك هذا على فهم المشكلة بطريقة أكثر شمولاً ويسمح لك بتصنيف المشكلات والاستجابة وفقًا لذلك. من الممكن تحديد نقاط الضعف التي تؤثر على عنصر واحد أو عناصر متعددة من ثالوث CIA. لاستخدام تطبيق ويب مع ثغرة SQL injection كمثال:

السرية: ثغرة SQL injection تسمح للمهاجم باستخراج المحتويات الكاملة لتطبيق الويب، مما يسمح له بالوصول الكامل لقراءة جميع البيانات، ولكن ليس لديه القدرة على تغيير المعلومات أو تعطيل الوصول إلى قاعدة البيانات.

النزاهة: ثغرة SQL injection تسمح للمهاجم بتغيير المعلومات الموجودة في قاعدة البيانات. لا يمكن للمهاجم قراءة البيانات أو منع الآخرين من الوصول إلى قاعدة البيانات.

التوفر: ثغرة SQL injection التي تبدأ استعلامًا طويل الأمد "long-running query"، وتستهلك قدرًا كبيرًا من الموارد على الخادم. يؤدي هذا الاستعلام، عند البدء عدة مرات، إلى حالة رفض الخدمة (DOS). ليس للمهاجم القدرة على الوصول إلى البيانات أو تغييرها ولكن يمكنه منع المستخدمين الشرعيين من الوصول إلى تطبيق الويب.

متعددة: تؤدي ثغرة SQL injection إلى وصول shell تفاعلي كامل إلى نظام التشغيل المضيف الذي يشغل تطبيق الويب. من خلال هذا الوصول، يمكن للمهاجم أن ينتهك سرية النظام عن طريق الوصول إلى البيانات كما يحلو لهم، ويهدد سلامة النظام عن طريق تغيير البيانات، وإذا اختاروا ذلك، قم بتدمير تطبيق الويب، مما يؤدي إلى اختراق في توفر النظام.

المفاهيم الكامنة وراء ثالوث CIA ليست معقدة للغاية، وواقعياً هي العناصر التي تعمل معها بشكل فطري، حتى إذا لم نتعرف عليها. ومع ذلك، من المهم أن نتفاعل مع هذا المفهوم بعناية حيث يمكن أن تساعدك على التعرف على مكان توجيه جهودك. سيساعدك هذا الأساس المفاهيمي في تحديد المكونات الأساسية لأنظمتك ومقدار الجهد والموارد التي تستحق الاستثمار في تصحيح المشكلات المحددة.

المفهوم الآخر الذي سنتناوله بالتفصيل هو المخاطر "*risk*"، وكيف تتكون من التهديدات "*threats*" ونقاط الضعف "*vulnerabilities*". هذه المفاهيم ليست معقدة للغاية، ولكن من السهل أن تخطئ. سنغطي هذه المفاهيم بالتفصيل لاحقًا، ولكن على مستوى عالٍ، من الأفضل التفكير في المخاطر على أنها ما تحاول منعه من الحدوث، والتهديد مثل من سيفعل ذلك بك، والضعف: ما يسمح لهم بذلك. يمكن وضع ضوابط للتعامل مع التهديد أو الضعف، بهدف التخفيف من المخاطر.

على سبيل المثال، عند زيارة بعض أنحاء العالم، قد تكون معرضًا *لخطر* الإصابة بالملاريا. وذلك لأن *تهديد* البعوض *مرتفع* للغاية في بعض البلدان، ومن المؤكد أنك لست محصنًا ضد الملاريا. لحسن الحظ، يمكنك التحكم في *الضعف* باستخدام الأدوية ومحاولة السيطرة على التهديد باستخدام طارد الحشرات والناموسيات. مع وجود ضوابط قائمة للتعامل مع كل من *التهديد والضعف*، يمكنك المساعدة في ضمان عدم تحقق *الخطر*.

١.١١. كالي لينكس في التقييم

عند الاستعداد لاستخدام Kali Linux في الميدان، يجب عليك أولاً التأكد من أن لديك تثبيتًا نظيفًا وفعالًا. من الأخطاء الشائعة التي يرتكبها العديد من محترفي الأمان المبتدئين استخدام تثبيت واحد عبر تقييمات متعددة. هذه مشكلة لسببين رئيسيين:

على مدار التقييم، غالبًا ما تقوم بتثبيت نظامك أو تعديله أو تغييره يدويًا. هذه التغييرات لمرة واحدة قد تجعلك تعمل بسرعة أو تحل مشكلة معينة، ولكن من الصعب تتبعها؛ تجعل نظامك أكثر صعوبة في الحفاظ عليه؛ وهي تعقد التكوينات المستقبلية.

كل تقييم أمني فريد من نوعه. يمكن أن يؤدي التخلف عن الملاحظات والتعليمات البرمجية والتغييرات الأخرى إلى الارتباك، أو ما هو أسوأ - التلوث المتبادل لبيانات العميل.

هذا هو السبب في أن البدء بتثبيت Kali نظيف موصى به بشدة ولماذا يكون لديك إصدار مخصص مسبقًا من Kali Linux جاهز للتثبيت التلقائي بسرعة. تأكد من الرجوع إلى القسم ٣.٩، "إنشاء صور ISO مخصصة لـ Kali Live" والقسم ٣.٤، "عمليات التثبيت غير المراقب" حول كيفية القيام بذلك، نظرًا لأنه كلما زادت أتمتة اليوم، قل الوقت الذي تضيعه غدًا.

لكل شخص متطلبات مختلفة عندما يتعلق الأمر بالطريقة التي يحبونها لتكوين Kali Linux عندما يكونون في العمل، ولكن هناك بعض التوصيات العالمية التي تريد اتباعها حقًا. أولاً، فكر في استخدام تثبيت مشفر كما هو موثق في القسم ٢.٢.٤، "التثبيت على نظام ملفات مشفر بالكامل". سيؤدي ذلك إلى حماية بياناتك على الجهاز المادي، وهو منقذ للحياة إذا سرق جهاز الحاسوب المحمول الخاص بك.

لمزيد من الأمان أثناء السفر، قد تحتاج إلى إدخال مفتاح فك التشفير (انظر إضافة كلمة مرور Nuke لمزيد من الأمان) بعد إرسال نسخة (مشفرة) من المفتاح إلى زميل في العمل في المكتب. بهذه الطريقة، تكون بياناتك آمنة حتى تعود إلى المكتب حيث يمكنك استعادة الحاسوب المحمول باستخدام مفتاح فك التشفير.

العنصر الآخر الذي يجب عليك التحقق منه هو قائمة الحزم التي قمت بتثبيتها. ضع في اعتبارك الأدوات التي قد تحتاجها للعمل الذي تحدده لإنجازه. على سبيل المثال، إذا كنت تشرع في تقييم أمان لاسلكي، فيمكنك التفكير في تثبيت ملف التعريف kali-linux-wireless، الذي يحتوي على جميع أدوات التقييم اللاسلكي المتاحة في Kali Linux، أو إذا كان تقييم تطبيق الويب قادمًا، يمكنك القيام بتثبيت جميع أدوات اختبار تطبيق الويب المتاحة باستخدام ملف التعريف kali-linux-web. من الأفضل أن تفترض أنك لن تتمكن من الوصول بسهولة إلى الإنترنت أثناء إجراء تقييم أمني، لذا تأكد من الاستعداد قدر الإمكان مسبقًا.

لنفس السبب، قد ترغب في مراجعة إعدادات الشبكة الخاصة بك (انظر القسم ١.٥، "تكوين الشبكة" والقسم ٣.٧، "تأمين خدمات الشبكة"). تحقق مرة أخرى من إعدادات DHCP وراجع الخدمات التي تستمع على عنوان IP المخصص لك. قد يكون لهذه الإعدادات تأثير حاسم على

نجاحك. لا يمكنك تقييم ما لا يمكنك رؤيته وقد تؤدي خدمات الاستماع المفرطة إلى وضع علامة "flag" على نظامك وإيقافه قبل البدء.

إذا كان دورك ينطوي على التحقيق في عمليات اختراق الشبكات، فإن الانتباه الدقيق لإعدادات الشبكة الخاصة بك هو أكثر أهمية وتحتاج إلى تجنب تغيير الأنظمة المتأثرة. لن تقوم نسخة مخصصة من Kali مع حزمة metapackage **kali-linux-forensic** التي تم تشغيلها في وضع التحقيق الجنائي بتثبيت الأقراص تلقائيًا أو استخدام قسم المبادلة. بهذه الطريقة، يمكنك المساعدة في الحفاظ على تكامل النظام قيد التحليل مع الاستفادة من العديد من أدوات التحقيق الجنائي المتاحة في Kali Linux.

من المهم أن تقوم بإعداد تثبيت Kali Linux بشكل صحيح لهذه المهمة. ستجد أن بيئة كالي النظيفة والفعالة ستجعل كل شيء يتبع المزيد من السلاسة دائمًا.

٢.١١. أنواع التقييمات

الآن بعد أن تأكدت من أن بيئة Kali الخاصة بك جاهزة، فإن الخطوة التالية هي تحديد نوع التقييم الذي تجريه بالضبط. على أعلى مستوى، يمكننا وصف أربعة أنواع من التقييمات: تقييم الضعف "*vulnerability assessment*"، واختبار الامتثال "*compliance test*"، واختبار الاختراق التقليدي، وتقييم التطبيق "*application assessment*". قد تتضمن المشاركة عناصر مختلفة من كل نوع من أنواع التقييم، ولكن من الجدير وصفها ببعض التفاصيل وشرح مدى صلتها ببناء وبيئة Kali Linux الخاصة بك.

قبل الخوض في الأنواع المختلفة من التقييمات، من المهم أن نلاحظ أولاً الفرق بين الضعف "vulnerability" والثغرة "exploit".

تُعرّف الثغرة "*vulnerability*" بأنها خلل، عند استغلالها، سيضر بسرية نظام المعلومات أو سلامته أو توفره. هناك العديد من أنواع الثغرات المختلفة التي يمكن مواجهتها، بما في ذلك:

- **تضمين الملف "File Inclusion":** تسمح لك ثغرات تضمين الملف في تطبيقات الويب بتضمين محتويات ملف محلي أو بعيد في البرنامج. على سبيل المثال، قد يحتوي تطبيق الويب على وظيفة "رسالة اليوم" التي تقرأ محتويات الملف وتضمينه في صفحة الويب لعرضه للمستخدم. عندما تتم برمجة هذا النوع من الميزات بشكل غير صحيح، يمكن أن يسمح للمهاجم بتعديل طلب الويب الخاص به لإجبار الموقع على تضمين محتويات ملف من اختياره.

حقن SQL "SQL Injection": هجوم حقن SQL هو هجوم حيث يتم تجاوز إجراءات التحقق من صحة الإدخال للبرنامج، مما يسمح للمهاجم بتوفير أوامر SQL للبرنامج المستهدف للتنفيذ. هذا شكل من أشكال تنفيذ الأوامر يمكن أن يؤدي إلى مشاكل أمنية محتملة.

تجاوز سعة المخزن المؤقت "Buffer Overflow": تجاوز سعة المخزن المؤقت هي ثغرة أمنية تتجاوز إجراءات التحقق من الإدخال لكتابة البيانات في الذاكرة المجاورة للمخزن المؤقت. في بعض الحالات، قد يكون هذا الموقع المجاور للذاكرة حاسمًا لتشغيل البرنامج المستهدف ويمكن التحكم في تنفيذ التعليمات البرمجية من خلال المعالجة الدقيقة لبيانات الذاكرة المكتوبة.

حالة السباق "Race Conditions": حالة السباق هي ثغرة تستفيد من تبعيات التوقيت في البرنامج. في بعض الحالات، يعتمد سير عمل البرنامج على تسلسل معين من الأحداث التي تحدث. إذا كان بإمكانك تغيير تسلسل الأحداث هذا، فقد يؤدي ذلك إلى ضعف.

إن برمجية الإستغلال "*exploit*" هي برمجيات تستغل -عند استخدامها- ثغرة معينة، على الرغم من أن الثغرات ليست كلها قابلة للإستغلال. نظرًا لأن برمجية الإستغلال يجب أن تغير العملية الجارية، مما يجبرها على اتخاذ إجراء غير مقصود، فقد يكون إنشاء برمجية الإستغلال معقدة. علاوة على ذلك، هناك عدد من تقنيات مكافحة الاستغلال في منصات الحوسبة الحديثة التي تم تصميمها بحيث تجعل من الصعب استغلال نقاط الضعف، مثل: منع تنفيذ البيانات " Data Execution Prevention" (DEP) وتوزيع مساحة العنوان العشوائي " Address Space Layout Randomization" (ASLR). ومع ذلك، لمجرد عدم وجود استغلال معروف علنًا لثغرة أمنية معينة، لا يعني عدم وجود واحدة (أو أنه لا يمكن إنشاؤه). على سبيل المثال، تبيع العديد من المؤسسات برمجيات استغلال تجارية لم يتم نشرها أبدًا، لذا يجب التعامل مع جميع الثغرات على أنها قابلة للإستغلال.

١.٢.١١. تقييم الضعف

تعتبر الثغرة نقطة ضعف يمكن استخدامها بطريقة ما للتهديد بسرية نظام المعلومات أو سلامته أو توفره. في تقييم الثغرات الأمنية، هدفك هو إنشاء جرد بسيط للثغرات المكتشفة في البيئة المستهدفة "*target environment*". إن مفهوم البيئة المستهدفة هذا مهم للغاية. يجب أن تتأكد من البقاء ضمن نطاق الشبكة المستهدفة لعميلك والأهداف المطلوبة. قد يؤدي التسلل خارج نطاق التقييم إلى انقطاع الخدمة أو خرق الثقة مع عميلك أو اتخاذ إجراء قانوني ضدك وصاحب العمل.

نظرًا لبساطته النسبية، غالبًا ما يتم الانتهاء من اختبار الضعف في بيئات أكثر نضجًا بشكل منتظم كجزء من إظهار العناية الواجبة. في معظم الحالات، يتم استخدام أداة تلقائية، مثل تلك الموجودة في تصنيف تحليل الثغرات "Vulnerability Analysis" وتطبيقات الويب " Web Applications" في موقع أدوات Kali وقائمة تطبيقات سطح المكتب Kali، لاكتشاف الأنظمة الحية في بيئة مستهدفة، وتحديد خدمات الاستماع، وسرد اكتشاف أكبر قدر ممكن من المعلومات مثل برنامج الخادم والإصدار والنظام الأساسي وما إلى ذلك.

ثم يتم التحقق من هذه المعلومات بحثًا عن التوقيعات المعروفة للمشكلات أو نقاط الضعف المحتملة. تتكون هذه التوقيعات من تركيبات نقاط البيانات التي تهدف إلى تمثيل المشكلات المعروفة. يتم استخدام نقاط بيانات متعددة، لأنه كلما زادت نقاط البيانات التي تستخدمها، كان التعريف أكثر دقة. يوجد عدد كبير جدًا من نقاط البيانات المحتملة، بما في ذلك على سبيل المثال لا الحصر:

إصدار نظام التشغيل: ليس من غير المألوف أن تكون البرامج ضعيفة على أحد إصدارات نظام التشغيل ولكن ليس على إصدار آخر. ولهذا السبب، سيحاول الماسح تحديد إصدار نظام التشغيل الذي يستضيف التطبيق المستهدف بأكبر قدر ممكن من الدقة.

مستوى التصحيح: في كثير من الأحيان، سيتم إصدار تصحيحات لنظام تشغيل لا تزيد من معلومات الإصدار، ولكنها لا تزال تغير طريقة استجابة الثغرة، أو حتى القضاء على الثغرة تمامًا.

بنية المعالج: تتوفر العديد من تطبيقات البرامج لبنى معالجات متعددة مثل Intel x86 و Intel x64 وإصدارات متعددة من ARM و UltraSPARC وما إلى ذلك. في بعض الحالات، لن توجد ثغرة إلا على بنية محددة، لذا فإن معرفة هذه المعلومات يمكن أن تكون حاسمة للتوقيع الدقيق.

إصدار البرنامج: يعد إصدار البرنامج المستهدف أحد العناصر الأساسية التي يجب التقاطها لتحديد الثغرة الأمنية.

سيتم استخدام هذه النقاط والعديد من نقاط البيانات الأخرى لإنشاء توقيع لجزء من فحص الثغرات الأمنية. كما هو متوقع، كلما زادت نقاط البيانات المطابقة، كلما كان التوقيع أكثر دقة. عند التعامل مع تطابقات التوقيع، يمكنك الحصول على بعض النتائج المحتملة المختلفة:

الإيجابي الحقيقي "True Positive": يتم مطابقة التوقيع ويجسد ثغرة حقيقية. هذه النتائج هي النتائج التي ستحتاج إلى متابعتها وتصحيحها، فهذه هي العناصر التي يمكن للأفراد الخبيثين الاستفادة منها لإيذاء مؤسستك (أو عميلك).

إيجابية كاذبة "False Positive": التوقيع مطابق، لكن المشكلة المكتشفة ليست ثغرة حقيقية. في التقييم، غالبًا ما تعتبر هذه ضوضاء ويمكن أن تكون محبطة للغاية. لن ترغب أبدًا في رفض الإيجابية باعتبارها إيجابية خاطئة دون التحقق من الصحة بشكل أكبر.

صحيح سلبي "True Negative": التوقيع غير مطابق وليس هناك ضعف. هذا هو السيناريو المثالي، والتحقق من عدم وجود ثغرة في الهدف.

سلبي كاذب "False Negative": التوقيع غير مطابق ولكن هناك ثغرة قائمة. بقدر ما هو إيجابي كاذب، فإن السلبية الكاذبة أسوأ بكثير. في هذه الحالة، توجد مشكلة ولكن الماسح لم يكتشفها، لذلك ليس لديك ما يشير إلى وجودها.

كما يمكنك أن تتخيل، فإن دقة التوقيعات مهمة للغاية للحصول على نتائج دقيقة. كلما زادت البيانات التي يتم توفيرها، زادت فرصة الحصول على نتائج دقيقة من الفحص الآلي القائم على التوقيع، وهذا هو السبب في أن عمليات المسح الموثقة غالبًا ما تكون معروفة جدًا.

باستخدام المسح المصادق عليه "authenticated scan"، سيستخدم برنامج المسح بيانات الاعتماد المقدمة للمصادقة على الهدف. وهذا يوفر مستوى أعمق من معرفة الهدف أكثر مما كان ممكنًا. على سبيل المثال، في الفحص العادي، قد تكتشف فقط معلومات حول النظام يمكن اشتقاقها من خدمات الاستماع والوظائف التي تقدمها. يمكن أن يكون هذا قليلًا من المعلومات في بعض الأحيان ولكن لا يمكن أن يتنافس مع مستوى وعمق البيانات التي سيتم الحصول عليها إذا قمت بالمصادقة على النظام وقمت بمراجعة شاملة لجميع البرامج المثبتة والتصحيحات المطبقة وعمليات التشغيل وما إلى ذلك. هذا النطاق الواسع من البيانات مفيد للكشف عن نقاط الضعف التي ربما لم يتم اكتشافها لولا ذلك.

يقدم تقييم الثغرات الذي تم إجراؤه جيدًا لمحة عن المشكلات المحتملة في المؤسسة ويوفر مقاييس لقياس التغيير بمرور الوقت. يعد هذا تقييمًا خفيفًا إلى حد ما، ولكن حتى الآن، ستجري العديد من المؤسسات عمليات فحص مؤتمتة للضعف تلقائيًا في غير ساعات العمل لتجنب المشاكل المحتملة خلال اليوم عندما يكون توافر الخدمة والنطاق الترددي في غاية الأهمية.

كما ذكرنا سابقًا، سيتعين على فحص الثغرات التحقق من العديد من نقاط البيانات المختلفة للحصول على نتيجة دقيقة. كل هذه الاختبارات المختلفة يمكن أن تخلق حمولة على النظام المستهدف وكذلك تستهلك عرض النطاق الترددي. لسوء الحظ، من الصعب أن تعرف بالضبط عدد الموارد التي سيتم استهلاكها على الهدف لأنها تعتمد على عدد الخدمات المفتوحة وأنواع الشبكات التي قد ترتبط بهذه الخدمات. هذه هي تكلفة إجراء المسح؛ ستشغل موارد النظام. من المهم عند تشغيل هذه الأدوات أن يكون لديك فكرة عامة عن الموارد التي سيتم استهلاكها ومقدار الحمل الذي يمكن أن يستغرقه النظام المستهدف.

Scanning Threads

تتضمن معظم ماسحات الثغرات الأمنية خيارًا لتعيين مؤشرات الترابط لكل عملية مسح "threads per scan"، وهو ما يعادل عدد عمليات الفحص المتزامنة التي تحدث في وقت واحد. سيكون لزيادة هذا الرقم تأثير مباشر على الحمل على منصة التقييم وكذلك الشبكات والأهداف التي تتفاعل معها. من المهم مراعاة ذلك أثناء استخدام هذه الماسحات. من المغري زيادة "threads" من أجل إكمال عمليات المسح بشكل أسرع ولكن تذكر زيادة الحمل الكبيرة المرتبطة بذلك.

عند الانتهاء من فحص الثغرات الأمنية، عادة ما يتم ربط المشكلات المكتشفة بمعرفات الصناعة القياسية مثل رقم CVE و EDB-ID وvendor advisories. يتم استخدام هذه المعلومات، بالإضافة إلى نقاط الضعف CVSS score، لتحديد تصنيف المخاطر. إلى جانب السلبيات الكاذبة (والإيجابيات الكاذبة)، تعد هذه المخاطر التعسفية من المشكلات الشائعة التي يجب أخذها في الاعتبار عند تحليل نتائج الفحص.

نظرًا لأن الأدوات الآلية تستخدم قاعدة بيانات للتوقيعات لاكتشاف الثغرات الأمنية، فإن أي انحراف طفيف عن التوقيع المعروف يمكن أن يغير النتيجة وكذلك صحة الثغرة الملحوظة. تشير الإيجابية الخاطئة بشكل غير واضح لثغرة غير موجودة، في حين أن السلبية الزائفة عمياء بشكل فعال عن الثغرة ولا تبلغ عنها. وبسبب هذا، غالبًا ما يُقال إن الماسح لا يقل جودة عن قاعدة التوقيع "signature rule base" الخاصة به. لهذا السبب، يوفر العديد من البائعين مجموعات توقيع متعددة: مجموعة قد تكون مجانية للمستخدمين ومجموعة أخرى باهظة الثمن إلى حد ما تكون أكثر شمولًا، والتي يتم بيعها بشكل عام للعملاء من الشركات.

المشكلة الأخرى التي غالبًا ما تصادف مع عمليات فحص الثغرات الأمنية هي صحة تقييمات المخاطر المقترحة. يتم تحديد تصنيفات المخاطر هذه على أساس عام، مع مراعاة العديد من العوامل المختلفة مثل مستوى الامتياز، ونوع البرنامج، والمصادقة المسبقة أو اللاحقة. اعتمادًا على بيئتك، قد تكون هذه التصنيفات قابلة للتطبيق أو لا يمكن تطبيقها، لذلك لا ينبغي قبولها بشكل عمياء. فقط أولئك الذين لديهم دراية جيدة في الأنظمة ونقاط الضعف يمكنهم التحقق بشكل صحيح من تصنيفات المخاطر.

على الرغم من عدم وجود اتفاق محدد عالميًا بشأن تصنيفات المخاطر، يوصى بنشر NIST Special 800-30 كخط أساس لتقييم تصنيفات المخاطر ودقتها في بيئتك. يحدد NIST SP 800-30 الخطر الحقيقي للضعف المكتشف على أنه مزيج من احتمالية الحدوث والتأثير المحتمل.

١١.٢.١.١. محتمل الحدوث "Likelihood of Occurrence"

وفقًا للمعهد الوطني للمعايير والتكنولوجيا " According to the National Institute of Standards and Technology" (NIST)، يعتمد احتمال حدوثه " likelihood of occurrence" على احتمال أن تهديدًا معينًا قادر على استغلال ثغرة معينة، مع تصنيفات محتملة منخفضة أو متوسطة أو عالية.

عالية: الخصم المحتمل يتمتع بمهارات عالية ودوافع عالية والتدابير التي تم وضعها للحماية من الضعف ليست كافية.

متوسط: يكون الخصم المحتمل متحمسًا وماهرًا ولكن التدابير التي وضعت للحماية من الضعف قد تعوق نجاحه.

منخفض: الخصم المحتمل غير ماهر أو يفتقر إلى الدافع وهناك تدابير قائمة للحماية ضد الضعف التي تكون فعالة جزئيًا أو كليًا.

٢.١.٢.١١. تأثير "Impact"

يتم تحديد مستوى التأثير من خلال تقييم مقدار الضرر الذي يمكن أن يحدث إذا تم استغلال الثغرة الأمنية المعنية أو الاستفادة منها بطريقة أخرى.

مرتفع "High": قد يؤدي استغلال الثغرة الأمنية إلى خسائر مالية كبيرة جدًا، أو إلحاق ضرر بالغ بمهمة المنظمة أو بسمعتها، أو حتى الإصابة الخطيرة، بما في ذلك الخسائر في الأرواح.

متوسط "Medium": قد يؤدي استغلال الثغرات الأمنية إلى خسائر مالية أو إلحاق الضرر بمهمة أو سمعة المنظمة أو إصابة بشرية.

منخفض "Low": الاستفادة من الضعف قد يؤدي إلى درجة ما من الخسارة المالية أو التأثير على مهمة وسمعة المنظمة.

١١.٢.١.٣. الخطر العام "Overall Risk"

بمجرد تحديد احتمالية حدوثها وتأثيرها، يمكنك عندئذٍ تحديد تصنيف الخطر العام، والذي يتم تعريفه على أنه دالة في التصنيفين. يمكن تصنيف الخطر العام على أنه منخفض أو متوسط أو مرتفع، مما يوفر إرشادات للمسؤولين عن تأمين وصيانة الأنظمة المعنية.

عالية: هناك حاجة قوية لتطبيق تدابير إضافية للحماية من الضعف. في بعض الحالات، قد يُسمح للنظام بمواصلة العمل ولكن يجب تصميم الخطة وتنفيذها في أقرب وقت ممكن.

متوسطة: هناك حاجة لاتخاذ تدابير إضافية للحماية من الضعف. يجب تنفيذ خطة لتنفيذ التدابير المطلوبة في الوقت المناسب.

منخفض: سيحدد مالك النظام ما إذا كان سيتم تنفيذ إجراءات إضافية للحماية من الضعف أو يمكنهم اختيار قبول الخطر بدلاً من ذلك وترك النظام دون تغيير.

١١.٢.١.٤. باختصار

مع وجود العديد من العوامل التي تشكل الخطر الحقيقي للثغرة المكتشفة، يجب استخدام تصنيفات المخاطر المحددة مسبقًا من إخراج الأداة فقط كنقطة بداية لتحديد الخطر الحقيقي على المؤسسة ككل.

يمكن أن توفر التقارير التي تم إنشاؤها بكفاءة من تقييم الثغرات الأمنية، عند تحليلها من قبل متخصص، أساسًا أوليًا للتقييمات الأخرى، مثل اختبارات اختراق الامتثال. على هذا النحو، من المهم فهم كيفية الحصول على أفضل النتائج الممكنة من هذا التقييم الأولي.

يعد Kali منصة ممتازة لإجراء تقييم الضعف ولا يحتاج إلى أي تكوين خاص. في قائمة تطبيقات Kali، ستجد العديد من الأدوات لتقييم الثغرات الأمنية في فئات جمع المعلومات وتحليل الثغرات الأمنية وتحليل تطبيقات الويب. توفر العديد من المواقع، بما في ذلك قائمة أدوات Kali Linux المذكورة أعلاه، وموقع Kali Linux Official Documentation، ودورة Metasploit Unleashed المجانية موارد ممتازة لاستخدام Kali Linux أثناء تقييم الثغرات الأمنية.

٢,٢,١١. اختبار اختراق الامتثال

النوع التالي من التقييم حسب درجة التعقيد هو اختبار الاختراق القائم على الامتثال "compliance". هذه هي اختبارات الاختراق الأكثر شيوعًا لأنها متطلبات مفروضة من الحكومة والصناعة بناءً على إطار الامتثال الذي تعمل المنظمة بأكملها بموجبه.

على الرغم من وجود العديد من أطر الامتثال الخاصة بالصناعة، إلا أن الأكثر شيوعًا هو معيار أمان بيانات صناعة بطاقات الدفع "Payment Card Industry Data Security Standard" (PCI DSS)، وهو إطار تمليه شركات بطاقات الدفع التي يجب على تجار التجزئة الذين يعالجون المدفوعات المستندة إلى البطاقات الالتزام بها. ومع ذلك، يوجد عدد من المعايير الأخرى مثل: أدلة التنفيذ الفني لأمن وكالة أنظمة المعلومات الدفاعية " Defense Information Systems

"Agency Security Technical Implementation Guides" (DISA STIG)، وبرنامج إدارة المخاطر والتفويض الفيدرالي " Federal Risk and Authorization Management Program" (FEDRAMP)، وقانون إدارة أمن المعلومات الفيدرالية " Federal Information Security Management Act" (FISMA)، وغيرها. في بعض الحالات، قد يطلب عميل الشركة تقييمًا، أو يطلب رؤية نتائج أحدث تقييم لأسباب مختلفة. سواء كانت مخصصة أو مفوضة، تسمى هذه الأنواع من التقييمات بشكل عام اختبارات الاختراق القائمة على الامتثال، أو ببساطة "تقييمات الامتثال -compliance assessments- " أو "فحوصات الامتثال -compliance checks-".

يبدأ اختبار الامتثال غالبًا بتقييم الضعف. في حالة تدقيق التوافق مع PCI، يمكن لتقييم الثغرة، عند إجراؤه بشكل صحيح، أن يلبي العديد من المتطلبات الأساسية، بما في ذلك: "٢. لا تستخدم الإعدادات الافتراضية لكلمات مرور النظام ومعلمات الأمان الأخرى "(على سبيل المثال، مع أدوات من فئة قائمة (Password Attacks، 11 ". قم باختبار أنظمة وعمليات الأمان بانتظام "(باستخدام أدوات من فئة تقييم قاعدة البيانات) وغيرها. بعض المتطلبات مثل "٩. تقييد الوصول المادي إلى بيانات حامل البطاقة "و" ١٢. لا يبدو أن الحفاظ على سياسة تتناول أمن المعلومات لجميع الموظفين "يخضعون لتقييم الضعف التقليدي القائم على الأدوات ويتطلبون المزيد من الإبداع والاختبار.

على الرغم من حقيقة أنه قد لا يبدو من السهل جدًا استخدام Kali Linux لبعض عناصر اختبار الامتثال، فإن الحقيقة هي أن Kali مناسب تمامًا في هذه البيئة، ليس فقط بسبب مجموعة واسعة من الأدوات المتعلقة بالأمان، ولكن نظرًا لبيئة ديبان مفتوحة المصدر التي تم بناؤها عليها، مما يسمح بتثبيت مجموعة واسعة من الأدوات. البحث عن مدير الحزم بكلمات رئيسية مختارة بعناية

من أي إطار عمل امتثال تستخدمه يكاد يكون من المؤكد أن يؤدي إلى نتائج متعددة. كما هو الحال، تستخدم العديد من المؤسسات Kali Linux كمنصة قياسية لهذه الأنواع الدقيقة من التقييمات.

٣.٢.١١. اختبار الاختراق التقليدي

أصبح اختبار الاختراق التقليدي عنصرًا يصعب تعريفه، حيث له العديد من التعريفات المختلفة، اعتمادًا على المساحة التي يعملون فيها. ويعود جزء من هذا الارتباك في السوق إلى حقيقة أن مصطلح "اختبار الاختراق" أصبح أكثر استخدامًا اختبار الاختراق القائم على الامتثال المذكور سابقًا (أو حتى تقييم الضعف) حيث، حسب التصميم، لا نتعمق كثيرًا في التقييم لأن ذلك يتجاوز الحد الأدنى من المتطلبات.

لأغراض هذا القسم، سنخطو جانبًا في المناقشة ونستخدم هذه الفئة لتغطية التقييمات التي تتجاوز الحد الأدنى من المتطلبات؛ التقييمات المصممة لتحسين الأمن العام للمنظمة بالفعل.

على عكس أنواع التقييم التي تمت مناقشتها سابقًا، لا تبدأ اختبارات الاختراق غالبًا بتعريف نطاق، ولكن بدلاً من ذلك هدف مثل "محاكاة ما يمكن أن يحدث إذا تعرض مستخدم داخلي للخطر" أو "تحديد ما سيحدث إذا تعرضت المنظمة لهجوم مركز من قبل طرف خبيث خارجي ". أحد الاختلافات الرئيسية بين هذه الأنواع من التقييمات هو أنها لا تجد الثغرات الأمنية وتتحقق منها فحسب، بل تستغل المشكلات المحددة لكشف السيناريو الأسوأ. بدلاً من الاعتماد فقط على مجموعات أدوات فحص الثغرات الأمنية، يجب عليك المتابعة مع التحقق من صحة النتائج من

خلال استخدام استغلالات أو اختبارات للقضاء على الإيجابيات الكاذبة وتبذل قصارى جهدك لاكتشاف الثغرات المخفية أو السلبيات الكاذبة. غالبًا ما ينطوي ذلك على استغلال الثغرات التي تم اكتشافها في البداية، واستكشاف مستوى الوصول الذي يوفره استغلال، واستخدام هذا الوصول المتزايد كوسيلة لهجمات إضافية ضد الهدف.

وهذا يتطلب مراجعة نقدية للبيئة المستهدفة إلى جانب البحث اليدوي والإبداع والتفكير من خارج الصندوق لاكتشاف سبل أخرى للضعف المحتمل واستخدام أدوات واختبارات أخرى خارج تلك التي تم العثور عليها بواسطة الماسحات الأكثر ثغرة. بمجرد الانتهاء من ذلك، غالبًا ما يكون من الضروري بدء العملية بأكملها مرة أخرى عدة مرات للقيام بعمل كامل.

حتى مع هذا النهج، ستجد غالبًا أن العديد من التقييمات تتكون من مراحل مختلفة. تسهل Kali العثور على برامج لكل مرحلة عن طريق قائمة Kali:

جمع المعلومات: في هذه المرحلة، تركز على التعلم قدر الإمكان حول البيئة المستهدفة. عادةً ما يكون هذا النشاط غير هجومي وسيظهر مشابهًا لنشاط المستخدم القياسي. ستشكل هذه الإجراءات الأساس لبقية التقييم وبالتالي يجب أن تكون كاملة قدر الإمكان. تحتوي فئة "جمع المعلومات" في Kali على عشرات الأدوات للكشف عن أكبر قدر ممكن من المعلومات حول البيئة التي يتم تقييمها.

اكتشاف الثغرات الأمنية "Vulnerability Discovery": غالبًا ما يطلق عليه "جمع المعلومات النشط -active information gathering-"، حيث لا تهاجم ولكن تشارك في سلوك المستخدم غير القياسي في محاولة لتحديد الثغرات الأمنية المحتملة في البيئة

المستهدفة. هذا هو المكان الذي سيتم فيه فحص الثغرات الذي تمت مناقشته سابقًا. ستكون البرامج المدرجة في فئات تحليل الثغرات الأمنية وتحليل تطبيقات الويب وتقييم قواعد البيانات والهندسة العكسية مفيدة لهذه المرحلة.

الاستغلال: مع اكتشاف نقاط الضعف المحتملة، تحاول في هذه المرحلة استغلالها للحصول على موطئ قدم في الهدف. يمكن العثور على أدوات لمساعدتك في هذه المرحلة في فئات تحليل تطبيق الويب وتقييم قاعدة البيانات وهجمات كلمة المرور وأدوات الاستغلال.

Pivoting and Exfiltration: بمجرد إنشاء موطئ قدم، يجب إكمال خطوات أخرى. غالبًا ما تكون تصعيد امتيازات لمستوى ملائم لتحقيق أهدافك كمهاجم، وتنتقل إلى أنظمة أخرى ربما لم تكن في متناولك من قبل، وتتخلص من المعلومات الحساسة من الأنظمة المستهدفة. ارجع إلى فئات هجمات كلمة المرور، وأدوات الاستغلال، والشم، والانتحال، وفئات ما بعد الاستغلال للمساعدة في هذه المرحلة.

إعداد التقارير: بمجرد اكتمال الجزء النشط من التقييم، يتعين عليك بعد ذلك توثيق الأنشطة التي تم إجراؤها والإبلاغ عنها. غالبًا ما تكون هذه المرحلة غير فنية مثل المراحل السابقة، ولكن من المهم للغاية ضمان حصول العميل على القيمة الكاملة من العمل المنجز. تحتوي فئة أدوات إعداد التقارير على عدد من الأدوات التي أثبتت فائدتها في مرحلة إعداد التقارير.

في أغلب الحالات، ستكون هذه التقييمات فريدة جدًا في تصميمها حيث ستعمل كل منظمة مع التهديدات والأصول المختلفة للحماية. يجعل Kali Linux قاعدة متعددة الاستخدامات لهذه الأنواع من التقييمات وهذا هو المكان الذي يمكنك فيه الاستفادة حقًا من العديد من ميزات تخصيص Kali Linux. ستحتفظ العديد من المنظمات التي تجري هذه الأنواع من التقييمات بإصدارات مخصصة للغاية من Kali Linux للاستخدام الداخلي لتسريع نشر الأنظمة قبل إجراء تقييم جديد.

غالبًا ما تتضمن التخصيصات التي تقوم بها المؤسسات لعمليات تثبيت Kali Linux الخاصة بها:

التثبيت المسبق للطرود التجارية بمعلومات الترخيص. على سبيل المثال، قد يكون لديك حزمة مثل ماسح الثغرات التجارية الذي ترغب في استخدامه. لتجنب الاضطرار إلى تثبيت هذه الحزمة مع كل إصدار، يمكنك القيام بذلك مرة واحدة وظهورها في كل عملية نشر لـ Kali تقوم بها.

شبكات اتصال افتراضية خاصة (VPN) تم تكوينها مسبقًا. هذه مفيدة جدًا في الأجهزة المتخلفة التي تسمح لك بإجراء تقييمات "داخلية بعيدة". في معظم الحالات، ستتصل هذه الأنظمة مرة أخرى بنظام يسيطر عليه المقيِّم، مما يؤدي إلى إنشاء نفق يمكن للمقيِّم استخدامه للوصول إلى الأنظمة الداخلية. يعد Kali Linux ISO of Doom مثالًا على هذا النوع الدقيق من التخصيص.

برامج وأدوات تم تطويرها مسبقًا مثبتة داخليًا. سيكون لدى العديد من المؤسسات مجموعات أدوات خاصة، لذا فإن إعدادها مرة واحدة في تثبيت Kali مخصص يوفر الوقت.

تكوينات نظام التشغيل التي تم تكوينها مسبقًا مثل تعيينات المضيف وخلفية سطح المكتب وإعدادات الوكيل وما إلى ذلك. العديد من مستخدمي كالي لديهم إعدادات محددة يرغبون

في تعديلها. إذا كنت ستقوم بإعادة نشر كالي على أساس منتظم، فإن التقاط هذه التغييرات أمر منطقي للغاية.

٤.٢.١١. تقييم التطبيق

في حين أن معظم التقييمات لها نطاق واسع، فإن تقييم التطبيق هو تخصص يركز بشكل ضيق على تطبيق واحد. أصبحت هذه الأنواع من التقييمات أكثر شيوعًا بسبب تعقيد التطبيقات الحرجة للمهمة التي تستخدمها المنظمات، والتي يتم إنشاء العديد منها داخليًا. يضاف تقييم التطبيق عادة إلى تقييم أوسع، كما هو مطلوب. تشمل التطبيقات التي يمكن تقييمها بهذه الطريقة، على سبيل المثال لا الحصر:

تطبيقات الويب: سطح الويب الأكثر شيوعًا للهجوم المواجه للخارج، تجعل تطبيقات الويب أهدافًا كبيرة لمجرد أنه يمكن الوصول إليها. في كثير من الأحيان، ستجد التقييمات القياسية مشاكل أساسية في تطبيقات الويب، ومع ذلك، فإن المراجعة الأكثر تركيزًا تستحق في الغالب الوقت لتحديد المشكلات المتعلقة بسير عمل التطبيق. يحتوي ملف التعريف kali-linux-web على عدد من الأدوات للمساعدة في هذه التقييمات.

تطبيقات سطح المكتب المترجمة "Compiled desktop applications": برنامج الخادم ليس الهدف الوحيد؛ تشكل تطبيقات سطح المكتب أيضًا سطحًا رائعًا للهجوم. في السنوات الماضية، كانت العديد من تطبيقات سطح المكتب مثل قارئات PDF أو برامج الفيديو المستندة إلى الويب مستهدفة بشكل كبير، مما أجبرها على النضج. ومع ذلك،

لا يزال هناك عدد كبير من تطبيقات سطح المكتب التي تعد ثروة من نقاط الضعف عند مراجعتها بشكل صحيح.

تطبيقات الهاتف المحمول "Mobile applications": مع زيادة انتشار الأجهزة المحمولة، ستصبح تطبيقات الهاتف المحمول أكثر بكثير من سطح الهجوم القياسي في العديد من التقييمات. هذا هدف سريع الحركة ولا تزال المنهجيات تنضج في هذا المجال، مما يؤدي إلى تطورات جديدة عملياً كل أسبوع. يمكن العثور على الأدوات المتعلقة بتحليل تطبيقات الهاتف المحمول في فئة قائمة Reverse Engineering.

يمكن إجراء تقييمات التطبيق بعدة طرق مختلفة. كمثال بسيط، يمكن تشغيل أداة مؤتمتة خاصة بالتطبيق مقابل التطبيق في محاولة لتحديد المشكلات المحتملة. ستستخدم هذه الأدوات المنطق الخاص بالتطبيق في محاولة لتحديد المشكلات غير المعروفة بدلاً من الاعتماد فقط على مجموعة من التوقيعات المعروفة. يجب أن تحتوي هذه الأدوات على فهم مدمج لسلوك التطبيق. مثال شائع على ذلك هو الماسح لضعف تطبيق الويب مثل Burp Suite، الموجه ضد تطبيق يحدد أولاً حقول الإدخال المختلفة ثم يرسل هجمات حقن SQL الشائعة إلى هذه الحقول أثناء مراقبة استجابة التطبيق لمؤشرات هجوم ناجح.

في سيناريو أكثر تعقيدًا، يمكن إجراء تقييم التطبيق بشكل تفاعلي إما في الصندوق الأسود أو الصندوق الأبيض.

تقييم الصندوق الأسود: تتفاعل الأداة (أو المُقيِّم "assessor") مع التطبيق بدون معرفة خاصة أو وصول يتجاوز معرف المستخدم العادي. على سبيل المثال، في حالة تطبيق ويب، قد يكون للمقيم حق الوصول فقط إلى الوظائف والميزات المتوفرة لمستخدم لم يقم بتسجيل الدخول إلى النظام. ستكون أي حسابات مستخدم مستخدمة هي الحسابات التي يمكن للمستخدم العام تسجيل الحساب فيها ذاتيًا. سيمنع هذا المهاجم من القدرة على مراجعة أي وظيفة متاحة فقط للمستخدمين الذين يحتاجون إلى إنشاءها بواسطة المسؤول.

تقييم الصندوق الأبيض: غالبًا ما يكون للأداة (أو المُقيِّم) حق الوصول الكامل إلى الكود المصدري، والوصول الإداري إلى النظام الأساسي الذي يقوم بتشغيل التطبيق، وما إلى ذلك. وهذا يضمن اكتمال مراجعة كاملة وشاملة لجميع وظائف التطبيق، بغض النظر عن مكان وجود هذه الوظيفة في التطبيق. المفاضلة مع هذا هو أن التقييم ليس بأي حال من الأحوال محاكاة للنشاط الضار الفعلي.

من الواضح أن هناك ظلال رمادية بينهما. عادةً ما يكون العامل الحاسم هو هدف التقييم. إذا كان الهدف هو تحديد ما سيحدث في حالة تعرض التطبيق لهجوم خارجي مركز، فمن المرجح أن يكون تقييم الصندوق الأسود هو الأفضل. إذا كان الهدف هو تحديد وإزالة أكبر عدد ممكن من المشكلات الأمنية في فترة زمنية قصيرة نسبيًا، فقد يكون نهج الصندوق الأبيض أكثر كفاءة.

في حالات أخرى، قد يتم اتباع نهج مختلط حيث لا يمتلك المقيم حق الوصول الكامل للكود المصدري لتطبيق للنظام الأساسي الذي يقوم بتشغيل التطبيق، ولكن يتم توفير حسابات المستخدمين من قبل المسؤول للسماح بالوصول إلى أكبر قدر ممكن من وظائف التطبيق.

كالي هو منصة مثالية لجميع أنواع تقييمات التطبيقات. في التثبيت الافتراضي، نتوفر مجموعة من الماسحات الخاصة بالتطبيقات المختلفة. للحصول على تقييمات أكثر تقدمًا، توجد مجموعة من الأدوات ومحررات المصدر وبيئات البرمجة النصية. قد تجد أقسام تطبيق الويب والهندسة العكسية في موقع أدوات Kali مفيدة.

٣.١١. إضفاء الطابع الرسمي على التقييم

عندما تكون بيئة Kali الخاصة بك جاهزة ونوع التقييم المحدد، فأنت جاهز تقريبًا لبدء العمل. خطوتك الأخيرة هي إضفاء الطابع الرسمي على العمل الذي يتعين القيام به. هذا أمر بالغ الأهمية، لأن هذا يحدد توقعات العمل، ويمنحك الإذن للقيام بما قد يكون نشاطًا غير قانوني بخلاف ذلك. سنقوم بتغطية ذلك على مستوى عالٍ، ولكن هذه خطوة معقدة جدًا وهامة، لذا من المحتمل أن ترغب في الرجوع إلى الممثل القانوني لمؤسستك للحصول على المساعدة.

كجزء من عملية إضفاء الطابع الرسمي، ستحتاج إلى تحديد قواعد المشاركة للعمل. يغطي هذا عناصر مثل:

ما هي الأنظمة المسموح لك بالتفاعل معها؟ من المهم التأكد من أنك لا تتدخل عن طريق الخطأ في أي شيء بالغ الأهمية لعمليات الأعمال.

في أي وقت من اليوم وما هي فترة الهجوم المسموح بها للتقييم؟ ترغب بعض المنظمات في تحديد الأوقات التي يمكن إجراء عمل التقييم فيها.

عندما تكتشف ثغرة محتملة، هل يُسمح لك باستغلالها؟ إذا لم يكن كذلك، ما هي عملية الموافقة؟ هناك بعض المنظمات التي تتخذ نهجًا محكمًا للغاية في كل محاولة استغلال، في حين أن منظمات أخرى ترغب في اتباع نهج أكثر واقعية. من الأفضل تحديد هذه التوقعات بوضوح قبل بدء العمل.

إذا تم اكتشاف مشكلة مهمة، كيف يجب معالجتها؟ في بعض الأحيان، ترغب المنظمات في إبلاغها على الفور، وإلا يتم معالجتها عادةً في نهاية التقييم.

في حالة الطوارئ، بمن يجب عليك الاتصال؟ من المهم دائمًا معرفة الشخص الذي يجب الاتصال به عند حدوث مشكلة من أي نوع.

من سيعرف عن النشاط؟ كيف سيتم إبلاغهم؟ في بعض الحالات، سترغب المؤسسات في اختبار الاستجابة للحوادث وأداء الكشف كجزء من التقييم. من الجيد دائمًا معرفة ذلك مسبقًا، لذلك تعرف ما إذا كان يجب أن تأخذ أي درجة من التخفي في نهج التقييم.

ما هي التوقعات في نهاية التقييم؟ كيف سيتم إبلاغ النتائج؟ اعرف ما نتوقعه جميع الأطراف في نهاية التقييم. تحديد الناتج هو أفضل طريقة لإرضاء الجميع بعد اكتمال العمل.

على الرغم من عدم اكتمالها، تمنحك هذه القائمة فكرة عن التفاصيل التي يجب تغطيتها. ومع ذلك، يجب أن تدرك أنه لا يوجد بديل للتمثيل القانوني الجيد. بمجرد تحديد هذه العناصر، تحتاج إلى الحصول على تفويض مناسب لإجراء التقييم، نظرًا لأن معظم النشاط الذي ستقوم به أثناء التقييم قد لا يكون قانونيًا بدون سلطة مناسبة من شخص لديه السلطة لمنح هذا الإذن.

مع كل ذلك، لا يزال هناك خطوة أخيرة ستحتاج إلى اتخاذها قبل بدء العمل: التحقق. لا تثق مطلقًا بالنطاق الذي قدمته - تحقق منه دائمًا. استخدم مصادر معلومات متعددة للتأكد من أن الأنظمة الموجودة ضمن النطاق مملوكة من قبل العميل وأن هذه الأنظمة يتم تشغيلها من قبل العميل أيضًا. مع انتشار الخدمات السحابية، قد تنسى المؤسسة أنها لا تمتلك الأنظمة التي توفر لها الخدمة. قد تجد أنه يجب عليك الحصول على إذن خاص من مزود الخدمة السحابية قبل بدء العمل. بالإضافة إلى ذلك، تحقق دائمًا من مجموعات عناوين IP. لا تعتمد على افتراض المؤسسة بأنهم يمتلكون مجموعات IP كاملة، حتى لو قاموا بتسجيل الخروج كأهداف قابلة للتطبيق. على سبيل المثال، لقد رأينا أمثلة للمنظمات التي تطلب تقييمًا لنطاق شبكة C بالكامل عندما كانت في الواقع تمتلك مجموعة فرعية فقط من هذه العناوين. من خلال مهاجمة مساحة عنوان الفئة C بالكامل، انتهى بنا الأمر بمهاجمة جيران شبكة المنظمة. تحتوي الفئة الفرعية لـ**OSINT Analysis** من قائمة **Information Gathering** على عدد من الأدوات التي يمكن أن تساعدك في عملية التحقق من الصحة هذه.

٤.١١. أنواع الهجمات

بمجرد أن يتم العمل، ما هي بعض أنواع الهجمات المحددة التي ستشنها؟ لكل نوع من أنواع الضعف تقنيات الاستغلال المرتبطة به. سيغطي هذا القسم مختلف فئات الثغرات التي ستتفاعل معها في أغلب الأحيان.

بغض النظر عن فئة الثغرات التي تبحث عنها، يجعل Kali من السهل العثور على هذه الأدوات واستغلالها. تنقسم قائمة Kali الموجودة على واجهة المستخدم الرسومية الخاصة بك إلى فئات للمساعدة في تسهيل العثور على الأداة المناسبة. بالإضافة إلى ذلك، يحتوي موقع Kali Tools على قوائم شاملة للأدوات المختلفة المتاحة في Kali، مرتبة حسب الفئة وتم وضع علامة عليها لسهولة التصفح. يحتوي كل إدخال على معلومات تفصيلية حول الأداة بالإضافة إلى استخدام المثال.

١.٤.١١. الحرمان من الخدمة "Denial of Service"

تستفيد هجمات رفض الخدمة من الضعف لإحداث خسارة في الخدمة، غالبًا من خلال تعطل العملية الضعيفة. تحتوي فئة **Stress Testing** في قائمة Kali Linux على عدد من الأدوات لهذا الغرض.

عندما يسمع الكثير من الناس مصطلح "هجوم رفض الخدمة"، فإنهم يفكرون على الفور في هجمات استهلاك الموارد التي يتم إرسالها من مصادر متعددة في وقت واحد ضد هدف واحد. ستكون هذه عبارة عن هجوم رفض الخدمات الموزع "*distributed* denial of services attack"، أو DDOS. نادراً ما تكون هذه الأنواع من الهجمات جزءًا من تقييم أمني محترف.

بدلاً من ذلك، غالبًا ما يكون رفض الخدمة المفرد هو نتيجة محاولة غير صحيحة لاستغلال ثغرة أمنية. إذا أطلق كاتب برمجية الإستغلال كودًا جزئيًا وظيفيًا، أو كود إثبات المفهوم "proof-of-concept" (POC) وتم استخدامه في هذا المجال، فقد يؤدي ذلك إلى حالة رفض الخدمة. حتى برمجية الإستغلال مشفرة بشكل صحيح قد تعمل فقط في ظروف محددة للغاية ولكنها تتسبب في رفض الخدمة في ظروف أقل. قد يبدو أن الحل هو فقط استخدام كود استغلال آمن ومختبر، أو كتابة كودك الخاص. حتى مع هذا الحل، لا توجد ضمانات وهذا يحد بشدة من المقيِّم، مما يتسبب في قيود غير ضرورية، مما يؤدي إلى تقييم أقل. بدلاً من ذلك، المفتاح هو الحل الوسط. تجنب كود PoC والاستغلالات غير المختبرة في هذا المجال وتأكد دائمًا من أن المحامي قد غطاه في الحوادث الأخرى.

عادة، لا يتم شن هجمات رفض الخدمة عمدا. ستعلن معظم أدوات الثغرات الآلية عن رفض ثغرات الخدمة على أنها مخاطر أقل نظرًا لأنه بينما يمكنك إزالة الخدمة من التشغيل، لا يمكن استغلال تلك الخدمة لتنفيذ التعليمات البرمجية. ومع ذلك، من المهم أن نتذكر أنه لم يتم نشر جميع برمجيات الإستغلال علنًا وقد يؤدي حجب الثغرة في رفض الخدمة إلى إخفاء تهديد أعمق وأكثر خطورة. قد يكون استغلال تنفيذ التعليمات البرمجية لرفض الخدمة معروفًا ولكن ليس عامًا. الفكرة هي، انتبه إلى الحرمان من الثغرات في الخدمة وشجع عميلك على تصحيحها بغض النظر عن تصنيف التهديدات (منخفض غالبًا).

٢.٤.١١. تلف الذاكرة "Memory Corruption"

يحدث تلف في الذاكرة عندما يتم تعديل موقع داخل مساحة ذاكرة العملية عن طريق الخطأ بسبب أخطاء البرمجة. عادة ما تؤدي أخطاء تلف الذاكرة إلى سلوك برنامج غير متوقع، ولكن في

كثير من الحالات، تسمح هذه الأخطاء بمعالجة ذاكرة العملية بطريقة يمكن من خلالها التحكم في تدفق تنفيذ البرنامج، مما يسمح بنشاط محدد من قبل المهاجم.

يشار إلى هذه الهجمات عادةً باسم تجاوزات المخزن المؤقت "buffer overflows"، على الرغم من أن هذا المصطلح هو تبسيط مفرط. الأنواع الأكثر شيوعًا من فساد الذاكرة تختلف اختلافًا كبيرًا عن بعضها البعض ولها أساليب وتقنيات خاصة بها مطلوبة للاستغلال الناجح.

تجاوز سعة المخزن المؤقت للمكدس "Stack Buffer Overflow": عندما يكتب برنامج ما المزيد من البيانات إلى المخزن المؤقت على المكدس أكثر من المساحة المتاحة له، يمكن أن تتلف الذاكرة المجاورة، مما يؤدي في كثير من الأحيان إلى تعطل البرنامج.

كومة الذاكرة المؤقتة "Heap Corruption": يتم تخصيص ذاكرة كومة الذاكرة المؤقتة في وقت التشغيل وعادة ما تحتوي على بيانات من برنامج التشغيل. تحدث تلف كومة الذاكرة المؤقتة عن طريق معالجة البيانات للكتابة فوق القائمة المرتبطة مؤشرات ذاكرة كومة الذاكرة المؤقتة.

تجاوز عدد صحيح "Integer Overflow": تحدث هذه تجاوزات عندما يحاول تطبيق إنشاء قيمة رقمية لا يمكن احتواؤها داخل مساحة التخزين المخصصة له.

تنسيق النصوص "Format String": عندما يقبل أحد البرامج إدخال المستخدم وتنسيقه دون التحقق منه، يمكن الكشف عن مواقع الذاكرة أو الكتابة فوقها، اعتمادًا على الرموز المميزة للتنسيق المستخدمة.

٣.٤.١١. نقاط ضعف الويب "Web Vulnerabilities"

نظرًا لحقيقة أن مواقع الويب الحديثة لم تعد صفحات ثابتة، ولكن بدلاً من ذلك تم إنشاؤها حيوية للمستخدم، فإن متوسط موقع الويب معقد للغاية. تستغل نقاط ضعف الويب هذا التعقيد في محاولة لمهاجمة منطق إنشاء الصفحة النهائية أو العرض التقديمي لزائر الموقع.

هذه الأنواع من الهجمات شائعة للغاية، حيث وصلت العديد من المنظمات إلى النقطة التي لديها القليل جدًا من الخدمات التي تواجهها خارجيًا. اثنان من أكثر أنواع هجمات تطبيقات الويب شيوعًا هما حقن SQL والبرمجة النصية عبر المواقع "cross-site scripting" (XSS).

حقن SQL: تستفيد هذه الهجمات من التطبيقات المبرمجة بشكل غير صحيح والتي لا تقوم بتعقيم إدخال المستخدم بشكل صحيح، مما يؤدي إلى القدرة على استخراج المعلومات من قاعدة البيانات أو حتى الاستيلاء الكامل على الخادم.

البرمجة النصية عبر المواقع: كما هو الحال مع حقن SQL، تنجم هجمات XSS عن التعقيم غير الصحيح لإدخال المستخدم، مما يسمح للمهاجمين بمعالجة المستخدم أو الموقع في تنفيذ التعليمات البرمجية في سياق جلسة المتصفح الخاصة بهم.

تطبيقات الويب المعقدة والغنية شائعة جدًا، حيث تقدم سطح هجوم مرحبًا للأطراف الخبيثة. ستجد عددًا كبيرًا من الأدوات المفيدة في فئة قائمة تحليل تطبيقات الويب و metapackage kali-linux-web.

٤.٤.١١. هجمات كلمة المرور

هجمات كلمة المرور هي هجمات ضد نظام مصادقة خدمة. غالبًا ما يتم تقسيم هذه الهجمات إلى هجمات كلمات المرور عبر الإنترنت وهجمات كلمات المرور غير المتصلة بالإنترنت، والتي ستجدها في فئة قائمة Password Attacks. في هجوم كلمة المرور عبر الإنترنت، تتم محاولة كلمات مرور متعددة ضد نظام تشغيل. في هجوم كلمة المرور دون اتصال، يتم الحصول على القيم المجزأة أو المشفرة لكلمات المرور ويحاول المهاجم الحصول على قيم نصية واضحة. الحماية من هذا النوع من الهجمات هي حقيقة أن العمل خلال هذه العملية مكلف حسابياً، مما يحد من عدد المحاولات التي يمكنك إجراؤها في الثانية. ومع ذلك، توجد حلول لهذا، مثل استخدام وحدات معالج الرسومات (GPUs) لتسريع عدد المحاولات التي يمكن إجراؤها. يحتوي ملف التعريف kali-linux-gpu على عدد من الأدوات التي تستفيد من هذه القوة.

في الغالب، تستهدف هجمات كلمات المرور كلمات المرور الافتراضية التي يوفرها البائع. نظراً لأن هذه القيم معروفة جيدًا، سيبحث المهاجمون عن هذه الحسابات الافتراضية، على أمل أن يكونوا محظوظين. تشمل الهجمات الشائعة الأخرى هجمات القاموس المخصصة حيث يتم إنشاء قائمة كلمات مصممة خصيصًا للبيئة المستهدفة، ثم يتم إجراء هجوم بكلمة مرور عبر الإنترنت ضد الحسابات الشائعة أو الافتراضية أو المعروفة حيث تتم محاولة كل كلمة بالتسلسل.

في التقييم، من المهم جدًا فهم العواقب المحتملة لهذا النوع من الهجمات. أولاً، غالبًا ما تكون صاخبة جدًا بسبب محاولات المصادقة المتكررة. ثانيًا، يمكن أن تؤدي هذه الهجمات غالبًا إلى حالة إغلاق الحساب بعد إجراء العديد من المحاولات غير الصالحة ضد حساب واحد. أخيرًا، غالبًا ما يكون أداء هذه الهجمات بطيئًا جدًا، مما يؤدي إلى صعوبة عند محاولة استخدام قائمة كلمات شاملة.

٥.٤.١١. الهجمات من جانب العميل

يتم تنفيذ معظم الهجمات على الخوادم، ولكن مع صعوبة الهجوم على الخدمات، تم تحديد أهداف أسهل. تأتي الهجمات من جانب العميل نتيجة لذلك، حيث سيستهدف المهاجم التطبيقات المختلفة المثبتة على محطة عمل أحد الموظفين داخل مؤسسة مستهدفة. تحتوي فئة قائمة أدوات الهندسة الاجتماعية على عدد من التطبيقات الممتازة التي يمكن أن تساعد في تنفيذ هذه الأنواع من الهجمات.

من الأفضل استغلال هذا النوع من الهجمات بواسطة هجمات Flash و Acrobat Reader و Java التي كانت شائعة جدًا في أوائل القرن الحادي والعشرين. في هذه الحالات، سيحاول المهاجمون طلب هدف لزيارة صفحة ويب ضارة. ستحتوي هذه الصفحات على كود متخصص من شأنه أن يؤدي إلى ثغرات أمنية في هذه التطبيقات من جانب العميل، مما يؤدي إلى القدرة على تشغيل تعليمات برمجية ضارة على نظام الأهداف.

من الصعب للغاية منع الهجمات من جانب العميل، حيث تتطلب قدرًا كبيرًا من تثقيف المستخدم، وتحديثات التطبيق المستمرة، وعناصر التحكم في الشبكة للتخفيف من المخاطر بشكل فعال.

٥.١١. ملخص

في هذا الفصل، ألقينا نظرة سريعة على دور كالي في مجال أمن المعلومات. ناقشنا أهمية التثبيت النظيف والفعال واستخدام التشفير قبل التوجه إلى الميدان لحماية معلومات عميلك، وأهمية التمثيل القانوني لحمايتك ومصالح عميلك.

مكونات CIA (السرية والنزاهة والتوافر) هي العناصر الأساسية التي ستركز عليها عند تأمين نظام كجزء من النشر القياسي أو الصيانة أو التقييم. سيساعدك هذا الأساس المفاهيمي في تحديد المكونات الأساسية لأنظمتك ومقدار الجهد والموارد التي تستحق الاستثمار في تصحيح المشكلات المحددة.

ناقشنا عدة أنواع من الثغرات الأمنية، بما في ذلك تضمين الملف، وحقن SQL، وتدفقات المخزن المؤقت، حالة السباق.

إن دقة التوقيعات مهمة للغاية للحصول على نتائج مفيدة لتقييم الضعف. كلما زادت البيانات التي يتم توفيرها، زادت فرصة الحصول على نتائج دقيقة من الفحص الآلي القائم على التوقيع، وهذا هو السبب في أن عمليات المسح الموثقة غالبًا ما تكون شائعة جدًا.

نظرًا لأن الأدوات الآلية تستخدم قاعدة بيانات للتوقيعات لاكتشاف الثغرات الأمنية، فإن أي انحراف طفيف عن التوقيع المعروف يمكن أن يغير النتيجة وكذلك صحة الثغرة الملحوظة.

ناقشنا أيضًا الأنواع الأربعة من التقييمات: تقييم الضعف، اختبار الامتثال، اختبار الاختراق التقليدي، وتقييم التطبيق. على الرغم من أن كل نوع من أنواع التقييم يستفيد من مجموعة أساسية من الأدوات، فإن العديد من الأدوات والتقنيات تتداخل.

إن تقييم الثغرات بسيط نسبياً مقارنة بأنواع التقييم الأخرى وغالبًا ما يتكون من جرد آلي للمشكلات المكتشفة في بيئة مستهدفة. ناقشنا في هذا القسم أن الثغرة هي خلل، عند استغلاله، سيضر بسرية أو سلامة أو توفر نظام المعلومات. نظرًا لأنه يعتمد على التوقيع، يعتمد هذا النوع من التقييم على التوقيعات الدقيقة ويمكن أن يقدم إيجابيات وسلبيات خاطئة. ستجد الأدوات الأساسية لهذا النوع من التقييم في فئات قائمة أدوات تحليل الثغرات وأدوات الاستغلال في Kali Linux.

تعتمد اختبارات الامتثال على المتطلبات التي تفرضها الحكومة والصناعة (مثل PCI DSS و DISA STIG و FISMA)، والتي تعتمد بدورها على إطار الامتثال. يبدأ هذا الاختبار عادةً بتقييم الضعف.

اختبار الاختراق التقليدي هو تقييم أمني شامل مصمم لتحسين الوضع الأمني العام للمؤسسة بناءً على بعض التهديدات الواقعية. يتضمن هذا النوع من الاختبار عدة خطوات (ينعكس من خلال بنية قائمة Kali Linux) ويتوج باستغلال الثغرات المحورية والوصول المحوري إلى الأجهزة والشبكات الأخرى داخل النطاق المستهدف.

تركز تقييمات التطبيق (عادةً الصندوق الأبيض أو الصندوق الأسود) على تطبيق واحد وتستخدم أدوات متخصصة مثل تلك الموجودة في فئات قائمة تحليل تطبيقات الويب وتقييم قاعدة البيانات والهندسة العكسية وأدوات الاستغلال.

نوقشت عدة أنواع من الهجمات بما في ذلك: الحرمان من الخدمة، الذي يكسر سلوك التطبيق ويجعله غير قابل للوصول؛ تلف الذاكرة، مما يؤدي إلى التلاعب في ذاكرة العملية، مما يسمح غالباً بتنفيذ كود المهاجم؛ هجمات الويب، التي تهاجم خدمات الويب باستخدام تقنيات مثل حقن SQL وهجمات XSS؛ وهجمات كلمات المرور، والتي غالباً ما تعزز قوائم كلمات المرور لمهاجمة بيانات اعتماد الخدمة.

التمرين الأول للفصل الحادي عشر - تقييمات أمن المعلومات

١. اشرح العلاقة والاختلاف بين الضعف "vulnerability" والإستغلال "exploit".
٢. اشرح الفرق بين الإيجابية الكاذبة والسلبية الكاذبة. أيهما أخطر؟ لماذا ا؟
٣. ما هو حقن SQL؟
٤. ما هو تجاوز سعة المخزن المؤقت؟
٥. ما هي حالة السباق؟
٦. ما هي الثغرة الأمنية في تضمين الملف؟

الإجابات:

١. فيما يتعلق بأمن المعلومات، فإن الثغرة هي نقطة ضعف يمكن الاستفادة منها من أجل المساس بسرية نظام المعلومات أو سلامته أو توفره. برمجيات الإستغلال هي برمجية صممت خصيصًا لالاستفادة من الثغرة.

٢. تحدث الإيجابية الخاطئة عندما يشير فحص الثغرة الأمنية إلى ثغرة أمنية ولا توجد ثغرة. يحدث سلبية كاذبة عندما لا يكتشف الفحص وجود ثغرة أمنية ويوجد واحد بالفعل. السلبية الكاذبة أكثر خطورة لأنه تم التغاضي عن الثغرة الأمنية.

٣. حقن SQL هو نوع من الثغرات الأمنية يحدث عندما لا يقوم تطبيق الويب بتعقيم إدخال المستخدم بشكل صحيح مما يسمح بمعالجة قاعدة البيانات الأساسية.

٤. تجاوز سعة المخزن المؤقت هو نوع من الثغرات الأمنية يحدث عندما يسمح خطأ برمجة لمدخلات المستخدم بالكتابة إلى الذاكرة خارج المساحة المخصصة له.

٥. حالة السباق هي نوع من الثغرات الأمنية يحدث عندما يستطيع المستخدم من خلال التوقيت الدقيق تغيير سلسلة من الأحداث لإنشاء ثغرة أمنية.

٦. يعد تضمين الملف نوعًا من الثغرات الأمنية يحدث عندما يسمح تطبيق الويب للمستخدم بإرسال إدخال إلى الملفات أو تحميل الملفات إلى خادم.

اختبار الشهادة للفصل الحادي عشر

١. أي مما يلي ليس جزءا من "ثالوث CIA":

- ☐ التوفر
- ☐ المعلومات
- ☐ السرية
- ☐ النزاهة
- ☐ التصنيف
- ☐ إمكانية الوصول
- ☐ المصادقة

٢. تمتلك المؤسسة خادم الويب الذي يدر الإيرادات بناءً على وقت التشغيل. أي من سمات الأمان التالية للنظام ستكون التركيز الأساسي للمؤسسة؟

- ○ السرية
- ○ النزاهة
- ○ إمكانية الوصول
- ○ التوفر

٣. تم العثور على خلل في خوارزمية التشفير يضعف نظام التشفير. أي من العناصر التالية لثالوت CIA تأثر بهذا؟

- السرية
- إمكانية الوصول
- المصادقة
- التصنيف

٤. أي من البرامج التالية يصف أفضل البرامج التي يمكن استخدامها للاستفادة من ضعف الأمان؟

- حالة السباق
- التصحيح "patch"
- استغلال
- الثغرة

٥. أي مما يلي (مستمد من احتمالية الحدوث والتأثير) يوفر إرشادات للمسؤولين عن تأمين الأنظمة المعنية وصيانتها؟

- الخطر العام
- الإلتزام
- الإنحراف
- تصيف الخصومة

٦. أي مما يلي يحدد المشكلات لكشف أسوأ سيناريو؟

- اختبار الإختراق
- تقييم الضعف
- تقييم التطبيق
- اختبار التوافق

٧. أي مما يلي يصف بشكل أفضل تقنية يتم استخدامها لاستهداف التطبيقات المختلفة المثبتة على محطة عمل أحد الموظفين داخل مؤسسة مستهدفة؟

- حجب الخدمة
- تلف الذاكرة
- هجوم من جانب العميل
- حقن SQL

الإجابات الصحيحة:

١. المعلومات، التصنيف، إمكانية الوصول، المصادقة.

٢. التوفر.

٣. السرية.

٤. الاستغلال

٥. الخطر العام

٦. اختبار الإختراق

٧. هجوم من جانب العميل

١٢ الطريق للأمام

تهانينا! نأمل أن تكون الآن أكثر دراية بنظام Kali Linux ولا يجب أن تخاف من استخدامه لأي تجربة قد تفكر فيها. لقد اكتشفت ميزاته الأكثر إثارة للاهتمام، ولكنك تعرف أيضًا حدودها والطرق المختلفة للتعامل مع هذه القيود.

إذا لم تضع جميع الميزات موضع التنفيذ، فاحتفظ بهذا الكتاب للأغراض المرجعية وقم بتحديث ذاكرتك عندما تكون على وشك تجربة ميزة جديدة. تذكر أنه لا يوجد أفضل من الممارسة (والمثابرة) لتطوير مهارات جديدة. حاول بجد، حيث يستمر مدربي الهجوم على الأمن في التكرار.

١.١٢. مواكبة التغييرات

مع التوزيع المتغير باستمرار مثل kali-rolling، فإن بعض أجزاء الكتاب ستصبح بالضرورة قديمة. سنبذل قصارى جهدنا لإبقائها محدثة (على الأقل للنسخة عبر الإنترنت) ولكن في معظم الأجزاء حاولنا تقديم تفسيرات عامة يجب أن تكون مفيدة لفترة طويلة قادمة.

ومع ذلك، يجب أن تكون مستعداً لتبني التغييرات وإيجاد حلول لأي مشكلة قد تظهر. من خلال الفهم الأفضل لكالي لينكس وعلاقته بدبيان، يمكنك الاعتماد على كل من مجتمعات كالي وديبيان ومواردهم العديدة (أجهزة تتبع الأخطاء، والمنتديات، والقوائم البريدية، وما إلى ذلك) عندما تتعثر.

لا تخف من تسجيل الأخطاء (انظر القسم ٣.٦، "تقديم تقرير خطأ جيد")! إذا كنت مثلي، في الوقت الذي تكمل فيه الخطوات التي ينطوي عليها تقديم تقرير خطأ جيد (ويستغرق الأمر بعض الوقت)، فستكون قد قمت بحل المشكلة أو على الأقل العثور على حل جيد. وبتسجيل الخطأ فعلياً، سوف تساعد الآخرين المتأثرين بالمشكلة.

٢.١٢. اظهار معرفتك المكتسبة حديثا

هل أنت فخور بمهاراتك الجديدة في Kali Linux؟ هل ترغب في التأكد من أنك تتذكر الأشياء المهمة حقًا؟ إذا أجبت بنعم على أحد هذه الأسئلة، فعليك التفكير في التقدم بطلب للحصول على برنامج Kali Linux Certified Professional.

إنها شهادة شاملة ستضمن أنك تعرف كيفية نشر واستخدام Kali Linux في العديد من حالات الاستخدام الواقعية. إنها إضافة لطيفة إلى سيرتك الذاتية وتثبت أيضًا أنك مستعد للمضي قدمًا.

٣.٢. المضي قدما

علمك هذا الكتاب الكثير من الأشياء التي يجب أن يعرفها أي مستخدم لـ Kali Linux، لكننا اتخذنا بعض الخيارات الصعبة لجعله قصيراً، وهناك العديد من المواضيع التي لم تتم تغطيتها.

١.٣.١٢. نحو إدارة النظام

إذا كنت تريد معرفة المزيد عن إدارة النظام، فلا يمكننا إلا أن نوصيك بالاطلاع على دليل مسؤول ديبان:

https://debian-handbook.info/get/

ستجد هناك العديد من الفصول التكميلية التي تغطي خدمات يونكس الشائعة التي تخطيناها بالكامل في هذا الكتاب. وحتى بالنسبة للفصول التي تم إعادة استخدامها في كتاب كالي، ستجد الكثير من النصائح التكميلية، لا سيما على نظام التغليف (الذي يتم تغطيته أيضًا على نطاق أوسع في أدنى مستوى له).

من الواضح أن كتاب ديبان يقدم مجتمع ديبان بشكل أعمق وطريقة تنظيمه. على الرغم من أن هذه المعرفة ليست حيوية، إلا أنها مفيدة حقًا عندما يكون عليك التفاعل مع المساهمين في ديبان، على سبيل المثال من خلال تقارير الأخطاء.

٢.٣.١٢. نحو اختبار الاختراق

ربما لاحظت الآن أن هذا الكتاب لم يعلمك اختبار الاختراق. لكن الأشياء التي تعلمتها لا تزال مهمة. أنت الآن جاهز للاستفادة بشكل كامل من قوة Kali Linux، أفضل إطار لاختبار الاختراق. ولديك مهارات لينكس الأساسية المطلوبة للمشاركة في تدريب Offensive Security.

إذا كنت تشعر أنك لست جاهزًا بعد لدورة مدفوعة، يمكنك البدء باتباع التدريب المجاني عبر الإنترنت Metasploit Unleashed هي أداة اختبار اختراق شائعة جدًا ويجب أن تعرفها إذا كنت جادًا بشأن خططك لتعلم اختبار الاختراق.

الخطوة المنطقية التالية هي اتباع اختبار الاختراق مع دورة Kali Linux عبر الإنترنت تقود الطريق إلى شهادة "محترف الأمن المعتمد -Offensive Security Certified Professional -". يمكن متابعة هذه الدورة التدريبية عبر الإنترنت بالسرعة التي تناسبك، ولكن الشهادة في الواقع اختبار صعب، وطول ٢٤ ساعة، في العالم الحقيقي، واختبار الاختراق العملي الذي يتم في شبكة VPN معزولة.

هل أنت على مستوى التحدي؟

تمرين الفصل ١٢ - تنفيذ حلول KALI

مشاريع نهاية الدورة - استخدام Aircrack-NG

١. قم ببناء مستودعك الخاص، واستضف نسخة محدثة من aircrack-ng عليه.
٢. تأكد من أن أي بناء تقوم بتشغيله يتضمن هذا المستودع وإصدار aircrack-ng المحدث.



مشاريع نهاية الدورة - ISO of Doom

١. تنفيذ Kali Linux ISO لـ Doom. استخدم نسخة سحابة من (azure, AWS). ليكون بمثابة الخادم البعيد.



مشاريع نهاية الدورة - أجهزة كالي والأتمتة

١. قم ببناء نقطة وصول باستخدام جهاز Raspberry Pi الذي يشغل Kali و hostapd.
٢. قم بإنشاء الحد الأدنى من USB الذي سيطلق المستجيب عند الإقلاع في الوضع المباشر.



المحتويات